DOCUMENT RESUME

ED 373 117 TM 022 046

AUTHOR Pechman, Ellen M.; And Others
TITLE Education Data Confidentiality: Two Studies. Issues in Education Data Confidentiality and Access and Compilation of Statutes, Laws, and Regulations Related to the Confidentiality of Education Data.
INSTITUTION National Center for Education Statistics (ED), Washington, DC.
REPORT NO ISBN-0-16-045075-6; NCES-94-635
PUB DATE Jul 94
NOTE 86p.; Prepared for the Steering Committee and the Technology, Dissemination, and Communications Committee of the National Forum on Education Statistics.
AVAILABLE FROM U.S. Government Printing Office, Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328.
PUB TYPE Legal/Legislative/Regulatory Materials (090)

EDRS PRICE MF01/PC04 Plus Postage.
DESCRIPTORS *Access to Information; Civil Liberties; *Confidentiality; *Court Litigation; Data Collection; *Educational Research; Elementary Secondary Education; *Federal Legislation; Freedom of Information; Information Management; Public Policy; School Districts; State Legislation; *Statistical Data; Telephone Surveys

ABSTRACT

Two studies were commissioned by the National Forum on Education Statistics to address concerns about the confidentiality and security of education data. The first, "Issues in Education Data Confidentiality and Access," by Ellen Pechman, Eileen O'Brien, Amy Hightower, and Angela Williams covers major court challenges, data collection issues germane to education, and trends anticipated to affect data confidentiality policy. A central theme derived from telephone interviews with 11 state and local managers and users of education data is that while automation of student data systems in schools, districts, and states is still in early stages, national guidelines and standards are needed to build in protection that ensures individual privacy and supports efficient data collection. The second paper, "Compilation of Statutes, Laws, and Regulations Related to the Confidentiality of Education Data," by Sonny S. Bloom, Jacqueline Hlavin, Julia Pelagatti, and David Banisar, contains a survey of 34 states, abstracts, and analysis of federal and state restrictions and stipulations regarding data confidentiality issues. (The first paper contains 13 references.) (SLD)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED 373 117

education

Education Data Confidentiality:

SCOPE OF INTEREST NOTICE
The ERIC Facility has assigned this document for processing to: TM
In our judgment, this document is also of interest to the Clearinghouses noted to the right. Indexing should reflect their special points of view. TR

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
☒ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy

NATIONAL CENTER FOR EDUCATION STATISTICS
NCES
NATIONAL COOPERATIVE EDUCATION STATISTICS SYSTEM
NATIONAL FORUM ON EDUCATION STATISTICS

TM022046

A Report by
the National Forum on
Education Statistics

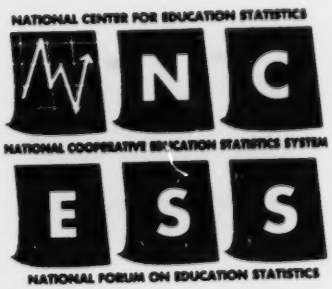
BEST COPY AVAILABLE

Education Data Confidentiality: Two Studies

Issues in Education Data Confidentiality and Access
and
Compilation of Statutes, Laws, and Regulations Related to the Confidentiality of Education Data

Prepared for the Steering Committee and the
Technology, Dissemination, and Communications Committee
of the National Forum on Education Statistics
under the National Center for Education Statistics,
U.S. Department of Education

July 1994



U.S. Department of Education
Richard W. Riley
Secretary

Office of Educational Research and Improvement
Sharon P. Robinson
Assistant Secretary

National Center for Education Statistics
Emerson J. Elliott
Commissioner

National Center for Education Statistics

"The purpose of the C[illegible]r shall be to collect, analyze, and disseminate statistic[illegible] and other data related to education in the United States and in other nations." —Section 406(b) of the General Education Provisions Act, as amended (20 U.S.C. 1221e-1).

July 1994

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328
ISBN 0-16-045075-6

Foreword

Recent and anticipated growth in the capacity of public agencies to collect, process, store, and report data electronically has created some public concern over data confidentiality and security. These issues were raised at the 1993 July Meeting of the National Forum on Education Statistics. In order to address these concerns and proactively set data confidentiality standards based on legal, ethical, and policy principles, the Forum commissioned two relevant studies to address the following issue questions:

- **Confidentiality.** What protections and assurances can be given to data respondents? What are the responsibilities and liabilities of data collectors?
- **Access.** Who has data access rights, under what circumstances, and for what purposes?
- **Security.** What constitutes adequate protection of data confidentiality?
- **Ownership.** Who owns data kept on individuals? Who has a legitimate voice in determining the use of such data?
- **Use.** What data may the private sector, the government, and other public agencies legitimately collect, and what is inappropriate? Under what conditions are responses for each data item considered mandatory or voluntary?

The two resulting studies are presented here. *Compilation of Statutes, Laws, and Regulations Related to the Confidentiality of Education Data* contains a survey, abstract, and analysis of federal and state restrictions and stipulations regarding data confidentiality issues. Its complement, *Issues in Education Data Confidentiality and Access*, covers major court challenges, data collection issues germane to education, and trends anticipated to affect data confidentiality policy. The Forum will use these studies as the basis for a plan of work to address data confidentiality standards in education.

Contents

Issues in Data Confidentiality and Access

Executive Summary 1

Introduction 3

Confidentiality and Data Access: A Timely Concern for the Forum 4

Data Collection for This Issue Brief 8

Summary of Findings 13

Proposed Plan of Work: Recommendations to the Forum Steering Committee 15

Bibliography 16

Attachment A: Private Lives and Public Policies—Confidentiality and Accessibility of Government Statistics 17

Attachment B: Summary of Interviews with Education Data Directors and Users 24

Compilation of Statutes, Laws, and Regulations Related to the Confidentiality of Education Data

I. Review 31
This section describes the modern use of privacy and confidentiality regarding individual records. It further describes the current federal laws, computer security, and how federal laws, statutes, and regulations interact.

Introduction 31
Preface 32
Hierarchy of Legal Requirements 33
Data Sharing 34
Data Security 35
Access to Computer Records and Systems 35
Electronic Mail 36

Overview of Major Federal Laws 36
Interrelationship of Three Laws 36
Law Coverage 37
Electronic vs. Physical Files 37

Contents, continued

Enforcement of Regulations and Penalties for Violation 37
School Policy on Record Access 38
Written Policy 38
Directory Information 39
Record Correction 39
Posting Student Information 39
Dissertations 39
Student Record Access Rights 40
Notification of Student Rights 40
Third-Party Access Rights 41
Exceptions to Third-Party Record Releases 41
Use of Social Security Numbers (SSN) 43

Conclusions 45

II. Matrix 47
The matrix outlines relevant federal laws, statutes, and regulations that affect privacy and confidentiality. It specifically addresses the information restricted, allowable communications, and release mechanisms among education and noneducation agencies.

III. Synopsis of Federal Laws 53
The synopsis gives a general guideline as to what each of the main federal laws encompasses in relation to data confidentiality, access, security, ownership, and use.

IV. State Laws 65
This section gives an overview of a few state laws that affect privacy and confidentiality, not only in education, but also in employment, health care, and general government agency business.

Appendix: Resources 73

BEST COPY AVAILABLE

Issues in Education Data Confidentiality and Access

Prepared for the
Steering Committee and the
Technology, Dissemination, and Communication Committee of the
National Forum on Education Statistics under the
National Center for Education Statistics, U.S. Department of Education

Ellen M. Pechman
Eileen O'Brien
Amy Hightower
Angela Williams

Policy Studies Associates, Inc.
1718 Connecticut Avenue, NW
Suite 400
Washington, DC 20009

BEST COPY AVAILABLE

Executive Summary

In November 1993, Policy Studies Associates (PSA) reviewed recent studies pertaining to data confidentiality and access and interviewed 11 state and local education data managers and users who work with data systems in nine states. The study coincided with the release of the National Academy of Sciences/National Research Council (NAS/NRC) report, *Private Lives and Public Policies*, an examination of current practices and new challenges in federal data collection and surveying that is a valuable resource for the National Forum on Education Statistics to consider as it plans its initiatives to safeguard education data collection, maintenance, and use.

The interviews with data managers confirmed that education data systems reflect a wide range of sophistication, and their attention to confidentiality and access issues is similarly varied. However, states and districts are adhering closely to standards established by the Family Education Rights and Privacy Act of 1974 (FERPA), as amended in 1988, as they institute electronic systems. Agencies typically have solid rules and regulations that both protect individual confidentiality and ensure adequate access for monitoring and policy planning. However, with greater reliance on electronic data systems and with the emergence of SPEEDE/ExPRESS, new issues regarding data confidentiality and access will arise. Key findings of the PSA study are:

- Currently, individual student data records are automated at the school or district levels; relatively few states electronically transfer data out of districts without prior aggregation. However, the cross-state data transfer anticipated by the Forum is still developing, so few states have needed to elaborate protective requirements beyond what is required under FERPA.
- Staff who work with student data are familiar with FERPA and other privacy protections. However, information is not readily available to taxpayers and interested citizens on how agencies maximize access while protecting individual rights and confidentiality when collecting data.
- Electronic data are regarded as more secure than paper files for maintaining and transferring student records because unauthorized access can be quickly detected and tracked on properly developed computer systems.
- With the increasing reliance on electronic data systems, implementation problems can be minimized if states and agencies develop coordinated guidelines, regulations, and procedures that protect against misuse of information or breaches of individual privacy.

The findings imply the need for the following activities which are consistent with other standard setting efforts of the Forum, including those developed for SEDCAR and SPEEDE/ExPRESS:

- **Prepare and disseminate easy-to-read documents** that explain current federal, state, and local privacy laws, indicating how student data and personnel records are routinely protected from breeches of privacy or inappropriate use.
- **Review and recommend guidelines on how to respond to potentially controversial issues** in electronic data management, such as (1) definitions of what data can be legally transferred across systems and states; (2) appropriate uses of Social Security numbers and other identifying codes; (3) decisionmaking about updating and deleting data from students' records; and (4) the applicability of federal privacy laws for state and local student data management and individual protection of privacy.
- **Establish standards based on recommendations in the NAS/NRC report,** *Private Lives and Public Policies,* and identify or develop model agreements, regulations, and assurances to disseminate to state education data managers, especially those initiating new electronic data systems.

Introduction

This issue brief reports the findings from a series of telephone interviews conducted by Policy Studies Associates (PSA) in November 1993 with 11 state and local data managers and users who work with education data systems in nine states. Its purpose is to present the central issues that this sample identified as their major concerns regarding current issues in education data confidentiality and access. In addition to the interviews, we consulted recently published sources that anticipate salient issues.

The central theme of this paper is that while automation of student data systems in schools, districts, and states is still in early developmental stages, national guidelines and standards are needed to build in protections that both ensure individual privacy and support efficient data gathering for education policy planning and decisionmaking. More comprehensive education data make possible improved evaluations that examine the trade-offs of competing policies and actions. However, if the source for such analyses is electronically transferred information about students, families, or school personnel, a tension emerges between social uses of data and the need to protect individuals.

The paper begins with a discussion of the context for concerns about data confidentiality and access in education statistics in an increasingly complex technological environment. It considers these issues in light of a recently issued national report resulting from a three-year study by the Panel on Confidentiality and Data Access of the U.S. Committee on National Statistics, a committee of the National Academy of Sciences and the National Research Council (NAS/NRC).[1] We then summarize the findings of PSA interviews with state and local education data managers and users. The paper concludes with recommendations for consideration by the National Forum on Education Statistics (Forum) and the National Center for Education Statistics (NCES).

[1] The Panel on Confidentiality and Data Access functioned under the auspices of the Committee on National Statistics and the Social Science Research Council of the National Research Council and the National Academy of Sciences. The Social Science Research Council is an autonomous, nongovernmental organization of social scientists from throughout the world. The Council's primary purpose is to advance the quality, value, and effectiveness of social science research.

Confidentiality and Data Access: A Timely Concern for the Forum

Education data are maintained within a federal and state legal framework of procedures for gathering and using student information for policymaking and reporting by schools and agencies.[2] Advances in technology and the wider use of education data for research and education planning have generated questions among individuals and advocacy groups about the degree to which existing and proposed databases are appropriately used. In particular, there are increasing concerns about the extent to which individual privacy rights and confidentiality are respected in data collection and maintenance and in research and reporting. Most recently, some political and religious groups have questioned whether the collection and use of individual student data for education program planning intrudes inappropriately into students' and families' private lives. On the other hand, the public is increasingly insistent that education agencies become more accountable for their use of public funds. Clearly, reliable and informed analyses of education achievement require more accurate and efficient data systems that describe students' participation and progress in educational programs.

In electronic data environments, it is especially important but increasingly difficult to define the line between privacy protection and inappropriate or inefficient limitation of use.

Aware of their obligations to protect individual privacy as they execute their data gathering responsibilities, government agencies have attempted to counteract potential privacy threats by restricting data access to a relatively limited core of users. However, while protecting individuals, the safeguards that are established also limit data use for worthwhile purposes, sometimes creating barriers that lead to governmental inefficiencies and frustrated statisticians and analysts who conduct policy research on behalf of the public. In electronic data environments, it is especially important but increasingly difficult to define the line between privacy protection and inappropriate or inefficient limitation of use.

Before the computerization of student data records, individual information about students and their families was typically under the control of teachers or principals and, occasionally, authorities in the judicial or social and health services who worked directly with students. Student records were rarely accessible beyond the school building or school district office. Today, complex computerized databases remove student information from the point of origin—the student, family, and school—and, in doing so, make data-driven education decisions increasingly available as policy-planning tools. At the student level, for example, test records can be combined to improve educators'

[2] Accompanying this issue brief is a companion paper, *Compilation of Laws, Statutes, and Regulations Related to the Confidentiality of Education Data*, summarizing key federal and state laws that guide data confidentiality and access procedures currently used by education agencies.

assessment of learning needs; at the policy level, combining individual student data with demographic, health, and parent information enables policymakers to determine strengths and weaknesses of key components of the education system; for fiscal planning, analyses of expenditures and outcome effects hold promise.

State and local education data agencies share with federal and state statistical agencies their awareness of the tenuous balance between access and privacy protection. These issues have been recently examined in depth in the NAS/NRC 3-year study, *Private Lives and Public Policies* (Duncan, Jabine, & Wolfe, 1993). The study was undertaken by the National Academy of Sciences Committee on National Statistics because of the pressing need for recommendations that aid federal statistical agencies in their "stewardship of data for policy decisions and research" (Duncan, et al., 1993, page 17).

It is appropriate that NCES and the Forum systematically examine education data collection processes and anticipate challenges, needs, and procedures created by electronic data collection systems for data collection and transfer. The findings of the NAS/NRC Panel on Confidentiality and Data Access (summarized in Attachment 1) offer national, state, and local education data agencies and users a valuable resource. However, the challenge of determining the right balance of competing public policy and individual privacy agendas within each agency remains up to the specific federal, state, or local agencies charged with specific data gathering responsibilities.

The Status of Electronic Data Gathering Systems in Education Agencies

Two reports recently summarized the progress state and local education agencies have made converting their student records from paper to electronic systems (Pallas, 1992; National Forum on Education Statistics, 1993). Responding to the recommendation of the Technical Planning Subgroup of the Resource Group for National Education Goal 2, High School Completion, Pallas surveyed the states to determine current practices and plans for developing a "Voluntary State/Local Student Record System." Pallas found the challenge of initiating statewide student record systems to be "fraught with difficulties." Systems are often developed with limited resources and knowledge; there is institutional uncertainty about the need for the data systems; and some educators and members of the public are concerned that comprehensive data systems will undermine local education authority. Pallas identified only nine states with fully integrated systems in place in 1991.

In the 1991-92 school year, NCES and members of the Forum's Technology, Dissemination, and Communication Committee conducted site visits to offer technical assistance to states that are automating their information management systems. The Forum (1993)

reported the status of data automation in 10 states and one regional agency,[3] summarizing current activities and issues and offering recommendations for next steps that would advance the implementation of their systems. For each state, the site visitors suggested specific actions and possible support that NCES or other states could offer. The striking finding of the Forum study is that states' approaches vary so widely that each state's political, technical, and resource issues make the implementation process unique to that state. As a result, matters anticipating confidentiality, privacy, and access were rarely mentioned in the reports of Forum site visitors.

PSA conducted its telephone interviews almost two years after the Pallas and Forum studies, and our sample cited gradual progress in the institutionalization of electronic record systems, but we also noted the same obstacles Pallas and the Forum found to the implementation of comprehensive, electronic student record systems. Furthermore, among the personnel we interviewed, only a few have tackled the issues of protection and access in sufficient depth to advise us either about procedures, complications or challenges they have encountered, or recommendations. There was, nonetheless, widespread agreement that investigating these issues and anticipating recommendations to guide state and local responses to confidentiality and access questions are appropriate priorities of a national advisory group such as the Forum.

Key Issues from the NAS/NRC Panel on Confidentiality and Data Access

The NAS/NRC Panel on Confidentiality and Data Access examined current practices and clarified new challenges in federal data collection and survey agencies. While recognizing the tension between data protection and data access, the Panel determined that it is possible to develop operational environments within agencies that enhance data access without decreasing data protection, and vice versa. Furthermore, their review of issues convinced panelists of the advisability of making recommendations for agencies to consider rather than attempt to make rules. Its resulting recommendations were based on three tenets about the use of information in a free society that reflect an inherent tension between data access and individual protection. These tenets are that:

[3] States included in this study are California, Colorado, Louisiana, Missouri, Nebraska, Nevada, Oregon, Tennessee, Washington, and Wisconsin. One regional agency, the Washington/Oregon Record Exchange, was also visited.

1. Democratic accountability recognizes the responsibilities of those who serve on behalf of others.
2. In the United States, the Constitution grants certain specific powers to a representative government, but at the same time it restrains executive excess and ensures broad access to the political process by its citizens.
3. Members of society are entitled to function as individuals, uncoerced and with privacy.

In the Panel's view, attending to these underlying principles makes it possible to provide recommendations without unnecessarily intruding in agency policymaking and planning. Its final report offered recommendations that are reasonable starting points for deliberations by NCES and the Forum Steering Committee.[4] Of the themes suggested by the NAS/NRC Panel, the following were also addressed by education agency personnel we interviewed in conjunction with this review of issues:

- Statutory protections
- Access to data and barriers to data sharing within government
- Privacy concerns and statistical procedures to protect confidentiality

[4] Attachment 1 summarizes the recommendations of the NAS/NRC Panel on Confidentiality and Data Access.

Data Collection for This Issue Brief

As part of this preliminary exploration of confidentiality and access issues in education data collection, PSA conducted telephone interviews with a limited number of state and local education officials, including data users, system developers, and policymakers. The telephone interviews were designed to focus on learning how the sample of states and local education agencies approach confidentiality and privacy issues; clarify controversial issues related to privacy and electronic data systems; and identify issues, policies, and practices in electronic data collection, access, and confidentiality.

We addressed the following key issues in the interviews:

- Status of electronic data collection
- Regulations and policies governing data collection and use
- Data access and security procedures
- Challenges regarding data access and confidentiality
- Recommendations for regulations, procedures, and guidance

The interview sample included 11 data managers in states, regions, or local education agencies with well-developed data systems, and those who manage programs that are beginning to implement integrated electronic data systems. More than half of the respondents were state-level officials, four were involved in data collection at the regional or local levels, and only one worked at the postsecondary level. The sites spanned all levels of electronic database sophistication, but the sample is small and selective, not representative. Further exploration of these themes is needed to confirm the initial findings that follow.

NCES staff and members of the Forum's Steering and Technology Committees proposed a preliminary list of potential interviewees. Those we contacted recommended additional individuals to talk with at the federal, state, and local levels, as well as representatives from elementary and secondary schools and postsecondary institutions.[5] We conducted the interviews in early November 1993. Time limitations required the project staff to focus on those interviewees we could reach during a brief, 3-week information-gathering period. While our sample is not representative either of education data agencies or users, it is sufficiently comprehensive to suggest directions for future study.

[5] Attachment B identifies the key respondents and summarizes the interview results. We also talked informally with representatives of the Department of Education's Family Policy Compliance Center, the NAS/NRC Committee on National Statistics, staff of the Panel on Confidentiality and Data Access, the Council of Chief State School Officers, and NCES.

The telephone interviews typically lasted between 30 minutes and an hour and informally explored the following topics:

- What individual student and personnel data are maintained on and transmitted through electronic systems?
- How are electronically maintained data being used by various educational agencies and systems? What governs their use?
- Who has access to individual data and data systems?
- How are data combined, transmitted, and reported to ensure confidentiality?
- What policies and procedures govern the use of student and personnel information?
- What issues regarding confidentiality of data collection and use have been raised in your institution or community? How did you deal with these issues and what would you recommend to others in similar situations?
- What do you think is the appropriate level of involvement in issues of confidentiality by local, state, or federal agencies?

We raised other issues of concern to NCES and the Forum—including students' right to know; involvement and conflicting interests of various groups in the decisionmaking process of data confidentiality policy; and authority to determine that data shall be collected, released, amended, or expunged—but these concerns were not immediately pressing to those we interviewed. In our opinion, the limited attention to this set of issues resulted not from their lack of salience, but, instead, that our interviews were relatively brief and our sample included too few individuals who were familiar with the legal technicalities of protection and access that data agencies face. Still, the respondents recognized that challenges on these matters constitute a potential threat to fragile systems that are in their earliest stages of development.

Still, data agencies very rarely establish methods for routinely publicizing confidentiality protections, so there appears to be little dissemination of information about FERPA protections and limitations on data use either within agencies or among the general public.

Themes that Emerged from Interviews

Status and Uses of Electronic Data Storage and Retrieval Systems

The level of sophistication in electronic data systems varies widely by state and district. Of those we interviewed, Iowa, Ohio, Washington, and Austin, Texas are highly automated. For example, both Washington and Ohio electronically collect and store a wide variety of student data (grade level, race, gender, legal residence, status of student, disability condition, LEP status, attendance, admission, withdrawal reasons, testing, including achievement test and proficiency test scores, course file, grades, disciplinary notes, etc.). In Iowa, Ohio, and Washington, intermediary agencies also

some districts in collecting and aggregating data before information is sent on to the state. By contrast, officials in Pennsylvania, Virginia, and Wyoming said that their states and their districts are not fully automated and students' individual records are not maintained at the state level.

Typically, states receive some data from their districts on computer disks or through modem transmissions and sometimes in paper reports. Most districts electronically collect and store basic demographic data (grade level, race, gender, disability condition, attendance, grades, disciplinary notes, etc.), but individual and aggregated analyses often depend on computer sophistication and willingness to apply scarce computer skills to these purposes.

Data are used for decisionmaking, measurement, planning, budget decisions, compliance with state and federal requirements, and requests from legislatures and councils. Several state managers acknowledged that access to individual student records (without names or any other identifiers) would streamline data reporting and decisionmaking that uses poverty indicators and academic progress information.

Regulations and Policies Governing Data Collection and Use

In general, interviewees reported that states or districts primarily relied on the Family Education Rights and Privacy Act of 1974 (FERPA) as amended in 1988 for guidance. According to our contacts, there is widespread understanding of state and local obligations to adhere to FERPA requirements and they have experienced few serious challenges to their procedures, either by data users or providers. Some states, such as Washington and Iowa, along with some districts, such as Austin, Texas, Montgomery County, Maryland, and San Diego Unified School District, California, went beyond FERPA to develop their own guidelines for added or more specific protection procedures. However, because neither states nor districts reported extensive procedures for monitoring compliance with confidentiality and privacy laws, it is unclear whether assumptions about systems' security are justified.

Most agencies that collect data report they have procedures in place to ensure that data users and managers are knowledgeable about FERPA and confidentiality protections. For example, a state administrator from Iowa noted that state department of education officials regularly meet with school representatives to discuss FERPA and confidentiality issues. An official from Arizona State University reported that data users must sign a form confirming that they have read and understand FERPA prior to receiving access to databases.

Still, data agencies very rarely establish methods for routinely publicizing confidentiality protections, so there appears to be little dissemination of information about FERPA protections and limitations on data use, either within agencies or among the general public. When asked, agency representatives reported that the protections of FERPA are accepted and few agencies see the need to make information about protections of

privacy more widely available. Austin was one of the few locales we learned about that put in place a comprehensive outreach to parents, regularly informing them of their rights regarding data collection. Arizona State University also periodically publicizes its privacy policies in the student newspaper and in the schedule of classes.

Access and Security

As states and districts develop their electronic databases and transmittal systems, concerns about putting student records on-line outweigh attention to procedures related to confidentiality and privacy. To protect the data, states routinely embed various levels of encrypted codes into their computerized databases and establish clear rules and procedures both about who can use data and the penalties for abuse or misuse of systems. In most cases, districts forward aggregated data, not original data, to the state, so state officials do not have access to individual records and access, and security of individual records becomes moot. The main exception to this procedure involves personnel records, such as teacher certification and salary information. Therefore, because district, not state, personnel control access to students' individual records, data security in states is not a priority concern. At the local levels, well-established rules emphasize individual student protection.

Most interviewees emphasize the distinction FERPA makes between "directory" information (e.g., student's name, address, age, and other basic demographics) and "record" information (grades, scores on standardized tests, and various personal information), using it as a model for setting up access and security procedures. The Montgomery County, Maryland, public school system gives teachers and other staff open access to "directory" information, but limits access to individual records to officials with appropriate security clearances.

The Washington (state) School Information Processing Cooperative offers software to its clients to help them limit information access to certain people. The system centers around password protection for different levels: some individuals are only allowed to read data, others may update data, others may use data for research and reporting, etc. Teachers can download information from the main computer to their desktop computer, if their school selected that option.

Ohio's data consortium also has a strong security system, with database access limited to those individuals with secured identification numbers. The system has internal monitoring devices that track and trace all accesses to the system, verifying the telephone numbers of any on-line terminal in the event of a security break-in attempt.

Interviewees reported few problems with unauthorized individuals accessing data, arguing that electronic data are typically more secure than a traditional paper system. Interviewees stressed that it is usually easier to monitor activity on a computer system than it is with file systems that are rarely maintained in adequately protected offices.

Challenges

In some states, proposed or actual use of Social Security numbers has led to controversy. Education officials would like student records to be easily identified for cross-identification, and a few state officials note that Social Security numbers are maintained to identify children in special education classes. However, officials from both California and Wyoming pointed out that this practice has caused some legal disputes. Resistance to linking student records to Social Security numbers recently developed so strongly in Virginia that schools no longer require a Social Security number for school registration.

An official with the Montgomery County, Maryland, schools questioned whether confidentiality concerns should affect file deletions. He sought guidance on the following questions: When do you delete information from a file? When does a discipline problem get cleared from a student's record? What information should be destroyed and when?

Another concern about data confidentiality was noted by a Virginia education official. Concerns about violence in the public schools led to a recent plan from the legislature, which calls for information on a student's criminal history to be added to his or her scholastic record. Supporters of the plan are concerned that the lack of coordination between the schools and the juvenile justice system could lead to juvenile offenders placing other students at risk, while opponents fear such recordkeeping could stigmatize a student. It is not clear whether such concerns exist in other states.

An additional potential area of concern is the application of FERPA rules to informal exchanges of information. Such exchanges typically occur during telephone conversations between people who know each other, and they often deal with referrals from school personnel to various social service or legal agencies and are limited to immediate problem solving. Yet we do not know the degree to which informal exchanges of information threaten confidentiality or privacy.

Summary of Findings

This study coincided with the release of the NAS/NRC report, *Private Lives and Public Policies*, an examination of current practices and new challenges in federal data collection and survey research. This report is a valuable resource for the Forum to consider as it plans its initiatives to safeguard education data collection, maintenance, and use.

Those we interviewed are concentrating on designing and implementing their electronic data systems. Numerous practical challenges are involved in establishing these systems within and across districts' records systems, only some of which are related to data security. Electronically maintained student records appear to be more private and offer better protection from misuse than paper files. Nevertheless, interviewees acknowledge that it is incumbent on their agencies to clarify the application of current federal and state laws for electronic data systems, explain monitoring procedures that ensure laws are followed, and disseminate the requirements for data use and sanctions for abuse of data systems. These findings were key:

- Currently, individual student data records are automated at the school or district levels; relatively few states transfer data out of the district electronically without prior aggregation. However, the cross-state data transfer anticipated by the Forum is just developing, so few states have needed to elaborate protective requirements beyond what is required under FERPA.
- As electronic data systems at all government levels become increasingly sophisticated and more widely used, security issues may need to be better understood and more closely monitored within agencies and districts.
- Among the potentially controversial issues that concern data management leaders are the following:
  1. Definitions of what data can be legally transferred across systems and states;
  2. Appropriate uses of Social Security numbers and other identifying codes;
  3. Decisionmaking about updating and deleting data from students' records; and
  4. The applicability of federal privacy laws for state and local student data management and individual protection of privacy.

Based on lessons from statistical agencies in other fields, managers in states and localities who are upgrading their electronic data systems are attentive to their responsibilities for informing in-house data providers and users of procedures that protect individual confidentiality and the integrity of data systems. Because they view themselves and their staffs as informed, the data managers we spoke with have relatively limited

concerns about the potential political problems associated with inadvertent breeches of privacy and confidentiality protections.

Not all data managers or users will be well prepared, however. Thus, there appears to be a need to inform those who work with electronic data and citizens as well as taxpayers of laws, regulations, and procedures that schools, states, and regional agencies adhere to in collecting, using, and protecting data confidentiality. Such information should be widely available, readable, and easily understood. It should summarize current federal and state assurances of privacy and limits on data access and use, and be accessible to the public through government agencies at local, state, and federal levels. These central findings are suggested:

- Standards, procedures, and recommendations are available from other agencies and from states that have established workable procedures, but there is relatively limited cross-agency or cross-state exchange, and wider dissemination of models would advance the security of new systems.
- States and other data agencies should be encouraged to inform agency personnel who work with personal record information—including student records, personnel records, and family demographic information—what regulatory restrictions limit access and use and encourage staff persons to make an effort to keep members of the public well informed of these rules, assurances, and routine protections of privacy.
- States, districts, and other data agencies need more routine procedures for publicizing widely across agencies and among taxpayers and citizens the confidentiality protections they have in place.

Proposed Plan of Work: Recommendations to the Forum Steering Committee

The data coordinated for this issue brief indicate that as state and local education agencies progress towards increasingly comprehensive electronic data systems, their managers recognize the potential challenges to confidentiality and problems of access that may occur as the use of and demand for information from the data systems increase. The findings from these interviews suggest that now is an appropriate time for NCES and the Forum to take the lead in tracking emergent issues, anticipate potentially controversial issues, and recommend standards, procedures, and regulations that ensure data confidentiality and access. Although neither states nor locales have thus far confronted debilitating challenges to their systems, the increased concerns about outcome-based education and student, teacher, and school accountability suggest an inevitable clash of values and priorities. Well-designed systems and well-informed managers and users in data agencies are the best insurance that the new programs will maximize their efficiency and usefulness for policy planning and decisionmaking while protecting the privacy of individuals.

Analyses conducted for this study suggest the following proposed plan of work the Forum Steering Committee may consider undertaking over the next several years. These suggested activities are consistent with previous standard-setting efforts of the Forum, including those developed for SEDCAR and SPEEDE/ExPRESS.

- **Prepare and disseminate easy-to-read documents** that explain current federal, state, and local privacy laws, indicating how student data and personnel records are routinely protected from breeches of privacy or inappropriate use.
- **Review and recommend guidelines on how to respond to potentially controversial issues** in electronic data management.
- **Establish standards based on recommendations in the NAS/NRC report,** *Private Lives and Public Policies,* and identify or develop model agreements, regulations, and assurances to disseminate to state education data managers, especially those initiating new electronic data systems.

Bibliography

California Department of Education. Policy Task Force on Confidentiality, Privacy, and Student Identification California Student Information System. (1993, September). *A Review of the Confidentiality, Privacy, and Security of Student Records in the Information Age in California.* Sacramento, CA: Author.

Cecil, J.S. (1993). Confidentiality legislation and the United States Federal Statistical System. *Journal of Official Statistics,* 9(2), 519-535.

Duncan, G.T., Jabine, B.T., & de Wolf, V.A. (Eds.) (1993). *Private Lives and Public Policies.* Washington, DC: National Academy Press.

Fienberg, S.E., Martin, M.E., & Straf, M.L. (Eds.) (1985). *Sharing Research Data.* Washington, DC: National Academy Press.

Jabine, T.B. (1993). Procedures for restricted data access. *Journal of Official Statistics,* 9 (2), 537-589.

Johnson, T.P. (1993, February 11). Managing student records: The courts and the Family Educational Rights and Privacy Act of 1974. *Education Law Reporter,* 1-18.

National Academy of Sciences. National Research Council. (1979). *Privacy and Confidentiality as Factors in Survey Response.* Washington, DC: Author.

North West Ohio Computer Association. Management Council of the Ohio Education Computer Network. (1992). *The Ohio Education Computer Network.* Archibald, OH: Author.

Pallas, A.M. (1992, March 26). *Statewide Student Record Systems: Current Status and Future Trends.* Washington, DC: National Education Goals Panel.

Reynolds, P.D. (1993). Privacy and advances in social and policy sciences: Balancing present costs and future gains. *Journal of Official Statistics,* 9 (2), 275-312.

San Diego Unified School District (1991). *New Beginnings Confidentiality Report.* San Diego, CA: Author.

U.S. Department of Education. National Center for Education Statistics. (1993, March). *SPEEDE/ExPRESS: An Electronic System for Exchanging Student Records.* Washington, DC: Author.

U.S. Department of Education. National Forum on Education Statistics. (1993, July). *Automated Information Management Systems: 11 Case Studies.* Washington, DC: Author.

Attachment A: Private Lives and Public Policies—Confidentiality and Accessibility of Government Statistics

Recommendations

The following recommendations emerged from the report of the NAS/NRC Panel on Confidentiality and Data Access, *Private Lives and Public Policies*, (Duncan et al.,1993, pp. 219-227). Three major areas concerned the panel primarily: protecting the interests of data subjects through procedures that ensure privacy and confidentiality; enhancing public confidence in the integrity of statistical and research data; and facilitating responsible dissemination to data users. The Panel's recommendations are organized by category, and they reflect the topics of each of the report's content chapters—Chapter 3: Data Subjects; Chapter 4: Data Users; Chapter 5: Legislation; Chapter 6: Technical and Administrative Procedures; Chapter 7: Statistical Data for Organizations; and Chapter 8: Managing Confidentiality.

Data Subjects

Recommendation 3.1

Federal statistical agencies should follow a flexible, multilayered approach to informing data providers of the conditions under which they are being asked to provide information.

Recommendation 3.2

Basic information given to all data providers requested to participate in statistical surveys and censuses should include:

(a) For data on persons, information needed to meet all Privacy Act requirements. Similar information is recommended for data on organizations, except that the requirement to inform providers about routine uses (as defined by the Privacy Act) is not applicable.

(b) A clear statement of the expected burden on the data providers, including the expected time requirement to provide the data (a requirement of the Office of Management and Budget) and, if applicable, the nature of sensitive topics included in the survey and plans for possible follow-up interviews of some or all respondents.

(c) No false or misleading statements. For example, a statement that implies zero risk or disclosure is seldom, if ever, appropriate.

(d) Information about any planned or potential *nonstatistical* uses of the information to be provided. There should be a clear statement of the level of confidentiality protection that can be legally ensured.

(e) Information about any planned or anticipated record linkages for statistical or research purposes. For persons, this notification will usually occur in conjunction with a request for the data subject's Social Security number.

(f) A statement to cover the possibility of unanticipated future uses of the data for statistical or research purposes.

(g) Information about the length of time for which the information will be retained in identifiable form.

Recommendation 3.3

Data subjects or data providers should be allowed to waive certain aspects of confidentiality protection that would usually be accorded to the information they provide. Agencies should take special care to ensure that any such waivers are based on fully informed consent.

Recommendation 3.4

Statistical agencies should undertake and support continuing research, using the tools of cognitive and survey research, to monitor the views of data providers and the general public on informed consent, response burden, sensitivity of survey questions, data sharing for statistical purposes, and related issues.

Recommendation 3.5

Federal statistical agencies should continue to develop systemic informational activities designed to inform the public of their ability to maintain the confidentiality of individually identifiable information, including use of legal barriers to disclosure and physical security procedures, and their intentions to minimize intrusion on privacy and the time and effort required to respond to statistical inquiries.

Recommendation 3.6

Agencies should be prepared to deal quickly and candidly with instances of "moral outrage" that may be directed at statistical programs from time to time as a result of actual or perceived violations of pledges of confidentiality given to data providers by data collectors. The agencies should be prepared to explain the purpose of specific data collection activities and the procedures used to protect the confidentiality. They should accept full responsibility if a violation occurs and should announce measures to prevent future violations.

Recommendation 3.7

As part of the communication process, statistical agencies should work more closely with appropriate advocacy groups, such as those concerned with civil liberties and those that represent the rights of disadvantaged segments of the population, and with specialists on ethical issues and human rights.

Data Users

Recommendation 4.1

Greater opportunities should be available for sharing of explicitly or potentially identifiable personal data among federal agencies for statistical and research purposes, provided the confidentiality of the records can be properly protected and the data cannot be used to make determinations about individual data subjects. Greater access should be permitted to key statistical and administrative data sets for the development of sampling frames and other statistical uses. Additional data sharing should only be undertaken in those instances in which the procedures for collecting the data comply with the panel's recommendations for informed consent or notification.

Recommendation 4.2

Federal statistical agencies should seek to improve the access of external users to statistical data, through both legislation and the development and greater use of tested administrative procedures under carefully controlled conditions.

Recommendation 4.3

All federal statistical agencies should establish systematic procedures for capturing information on a continuing basis about user requests for data that have been denied or only partially fulfilled. Such information should be used for periodic reviews of agency confidentiality and data access policies.

Recommendation 4.4

All users of federal data, regardless of the formal conditions of access, should subscribe to the following principles for responsible data use:

(a) Observe all conditions agreed to in order to obtain access to the data and allow access to the original data set only to those permitted access under the agreed conditions of recipiency, and ensure that all such persons are aware of the required conditions of use.

(b) Make no attempt to identify particular individuals or other units whose data are considered to be confidential.

(c) In the event that one or more individuals or other units are identified in the course of research, notify the organization that provided the data set, and do not inform anyone else of the discovered identities.

Recommendation 4.5

To promote knowledge of and adherence to the principles of responsible data use:

(a) Federal agencies should ask all recipients of federal microdata sets to submit to the releasing agency, in writing, their agreement to observe the above principles, plus any other conditions deemed necessary for specific data sets.

(b) Professional societies and associates that have ethical codes, standards, or guidelines should incorporate these principles in them.

(c) The principles and the justifications for them should be included in academic and other training for disciplines whose members are likely to be users of federal statistical data.

Legislation

Recommendation 5.1

Statistical records across all federal agencies should be governed by a consistent set of statutes and regulations meeting standards for the maintenance of such records, including the following features of fair statistical information practices:

(a) A definition of statistical data that incorporates the principle of functional separation as defined by the Privacy Protection Study Commission.

(b) A guarantee of confidentiality for data.

(c) A requirement of informed consent or informed choice when participation in a survey is voluntary.

(d) A requirement of strict control on data dissemination.

(e) A requirement to follow careful rules on disclosure limitation.

(f) A provision that permits data sharing for statistical purposes under controlled conditions.

(g) Legal sanctions for those who violate confidentiality requirements.

Recommendation 5.2

Zero-risk requirements for disclosure of statistical records are, in practice, impossibly high standards. Regulations and policies under existing statutes should establish standards of reasonable care. New statutes should recognize that almost all users of information entail some risk of disclosure and should allow release of information for legitimate statistical purposes that entail a reasonably low risk of disclosure of individually identifiable data.

Recommendation 5.3

There should be legal sanctions for all users, both external users and agency employees, who violate requirements to maintain the confidentiality of data.

Technical and Administrative Procedures

Recommendation 6.1

The Office of Management and Budget's Statistical Policy Office should continue to coordinate research work on statistical disclosure analysis and should disseminate the results of this work broadly among statistical agencies. Major statistical agencies should

actively encourage and participate in scholarly statistical research in this area. Other agencies should keep abreast of current developments in the application of statistical disclosure limitation techniques.

Recommendation 6.2

Statistical agencies should determine the impact on statistical analyses of the techniques they use to make data. They should be sure that the masked data can be accurately analyzed by a range of typical researchers. If the data cannot be accurately analyzed using standard statistical software, the agency should make appropriate consulting and software available.

Recommendation 6.3

Each statistical agency should actively involve data users from outside the agency as statistical disclosure limitation techniques are developed and applied to data.

Recommendation 6.4

Statistical agencies should continue widespread release, with minimal restrictions on use, of microdata sets with no less detail than currently provided.

Recommendation 6.5

Federal statistical agencies should strive for a greater return on public investment in statistical programs through carefully controlled increases in interagency data sharing for statistical purposes and expanded availability of federal data sets to external users.

Recommendation 6.6

Federal statistical agencies, in their efforts to expand access for external data uses, should follow a policy of responsible innovation. Whenever feasible, they should experiment with some of the newer restricted access techniques, with appropriate confidentiality safeguards and periodic reviews of the sets and benefits of each procedure.

Recommendation 6.7

In those instances in which controlled access at agency sites remains the only feasible alternative, statistical agencies should do all they can to make access conditions more affordable and acceptable to users (for example, by providing access at dispersed agency locations and providing adequate user support and access to computing facilities at reasonable costs).

Recommendation 6.8

Significant statistical data files, in their unrestricted form, should be deposited at the National Archives and eventually made available for historical research uses.

Statistical Data for Organizations

Recommendation 7.1

The principle of functional separation in Recommendation 5.1 (a) should apply equally to data for persons and data for organizations.

Recommendation 7.2

Legislation that authorizes and requires protection of the confidentiality of data for persons and organizations should be sought for all federal statistical agencies that do not now have it and for any new federal statistical agencies that may be created.

Recommendation 7.3

Data providers, whether persons or organizations, should have ready access to as much information as they want about the uses of the information they are requested or required to provide to federal statistical agencies. They should be told who will have access to their data in individually identifiable form. Statements of the collecting agency's intentions should be clearly distinguished from statements describing what is authorized and required by statute.

Recommendation 7.4

There should be increased sharing of business lists for statistical purposes by federal and state agencies.

Recommendation 7.5

New legislation on sharing of business lists for statistical purposes should provide that government agencies that are now unable to guarantee protection against nonstatistical uses can have access to business lists if they acquire statutory authority for such protection in the future.

Recommendation 7.6

The Office of Management and Budget's Statistical Policy Office should develop uniform guidelines for federal statistical agencies covering the purposes for which waivers of confidentiality protections by organizations reconsidered acceptable and the methods of obtaining waivers from respondents. Efforts should be made to amend the confidentiality statutes of federal statistical agencies that would otherwise be prevented from using waivers for generally accepted statistical purposes.

Recommendation 7.7

Federal statistical agencies that collect data on organizations should make a special effort to improve the access for statistical research and analysis by external users and, if necessary, should seek legislation that will permit them to develop licensing arrangements that allow such users to have access at their work sites, subject to penalties, for violating the conditions under which they are allowed to access to the data.

Managing Confidentiality and Data Access Functions

Recommendation 8.1

Each federal statistical agency should review its staffing and management of confidentiality and data access functions, with particular attention to the assignment within the agency of responsibilities for these functions and the background and experience needed for persons who exercise these responsibilities.

Recommendation 8.2

Statistical agencies should take steps to provide staff training in fair information practices, informed consent procedures, confidentiality laws and policies, statistical disclosure limitation procedures, and related topics.

Recommendation 8.3

Statistical agencies should establish mechanisms for allowing and encouraging greater external inputs into their decisions on confidentiality protection and data access.

Recommendation 8.4

The Statistical Policy Office should give high priority to proceeding with the development and issuance of the OMB *Guidelines for Statistical Activities*, with the full participation of the federal statistical agencies and the public.

Recommendation 8.5

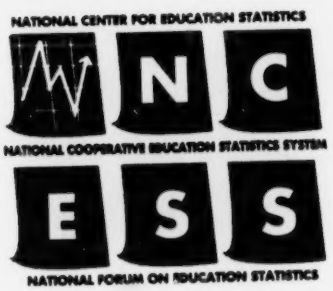
The panel supports the general concept of an independent federal advisory body charged with fostering a climate of enhanced protection for all federal data about persons *and* responsible data dissemination for research and statistical purposes. Any such advisory body should promote the principle of functional separations and have professional staff with expertise in privacy protection, computer databases, official statistics, and research uses of federal data.

Attachment B

Summary of Interviews with Education Data Directors and Users

State	Name/role	Organizational level of interviewee	Description of data system	Major concerns
Arizona	Mary Neary, Arizona University Assoc. Registrar	University	Student data electronically stored; security measures are in place	None
Iowa	Leland Tack, Administrator Division of Finances and Informational Services	State Dept. of Education	Personnel, financial, and student [spec. ed] data electronically stored at state level	Need private/ public clarification, use of SS# as identifiers, dissemination
Maryland	Joseph Hawkins, Evaluation Specialist	District: Montgomery County	Student data electronically stored at district level, some schools electronically connected	Maintaining and updating files; when and what info should be deleted from file
NW Ohio	Dwain Baker, Regional Director	Regional center	Student data electronically stored at regional level, security measures are in place	Dissemination
Ohio	Matt Cohen, Director of Policy Research	State Dept. of Education	Aggregated student data electronically collected at state level	Laws needed to guide electronic transfer of data
Pennsylvania	Roger Hummel, Chief of Data Services	State Dept. of Education	Student, financial, and personnel data electronically stored at state level	Use of SS#'s

State	Name/role	Organizational level of interviewee	Description of data system	Major concerns
Texas	Glenn Ligon, Consultant	Local service center	Electronic systems	Disaggregating data; clarification of the federal, state, and local regulations
Virginia	Cameron Harris, Division Chief for Information Services	State Dept. of Education	Very little collected electronically, aggregated student data stored at state level	Recommend federal guidance on the use of SS#'s and transfer of information across districts
Washington	Ed Strozyk, Database Manager, Washington Information Services	State Dept. of Education	Aggregated student data electronically stored at state level	Federal and state guidelines for policymaking
Washington	Jill Hanson, Washington School Information	Processing Cooperative	Regional service center	Electronic systems Dissemination
Wyoming	Steven King, Facilitator Data Utilization	State Dept. of Education	Beginning stages of electronically collecting aggregated student data at the state level	More flexibility for data use


NATIONAL CENTER FOR EDUCATION STATISTICS
NCES
NATIONAL COOPERATIVE EDUCATION STATISTICS SYSTEM
NATIONAL FORUM ON EDUCATION STATISTICS

Compilation of Statutes, Laws, and Regulations Related to the Confidentiality of Education Data

Prepared for the
Steering Committee and the
Technology, Dissemination, and Communication Committee of the
National Forum on Education Statistics under the
National Center for Education Statistics, U.S. Department of Education

Sonny S. Bloom
Jacqueline Hlavin
Julia Pelagatti
David Banisar

Rii
1010 Wayne Avenue
Suite 300
Silver Spring, MD 20910

I. Review

Introduction

The purpose of this report is to provide an overview of federal and state laws that affect individuals' personal data confidentiality and privacy, both as students and as employees, in the education environment. Our study efforts first encompassed legal research of the following federal laws: Privacy Act, Family Educational Rights and Privacy Act, Freedom of Information Act, Computer Matching Act, and others. We then progressed to reviewing relevant state laws, ultimately covering 34 states. Each reviewed state had a different type and extent of privacy or confidentiality coverage. For example, some states, such as California, are very detailed in regard to protection of records, while other states protect only communications between students and school counselors. We also conducted interviews with experts at the federal level (meeting with employees of the Internal Revenue Service, the Department of Justice, the Office of Personnel Management, and the Office of Consumer Affairs), the private sector (such as the *Privacy Journal*), and various other privacy organizations.

The following summary provides an overview of the key issues these laws address, while the subsequent sections of the report summarize the result of our legal research into specific federal and state laws.

Preface

Legal protections of privacy have existed for several centuries. The privacy of one's papers was upheld in English courts as far back as 1765, where Lord Camden, striking down a warrant to enter a house and seize papers, wrote, "We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have."[1]

The Constitution of the United States does not specifically enumerate a right of privacy. However, the U.S. Supreme Court has recognized the right to privacy and, through the years, it has been litigated and refined. The right of privacy has been found to be guaranteed under the prenumbra of the Constitution. In addition, the U.S. Senate ratified the International Covenant on Civil and Political Rights in 1992, which guarantees a right to privacy. This essentially means that through the vehicle of an international treaty each individual is guaranteed the right to privacy. There are various sources of law which are recognized and accepted as part of the Constitution. Foreign treaties are included among these sources.

The right to privacy has not been solely a federal issue. Some states include an explicit right to privacy in their constitution—for example, Hawaii,[2] Washington,[3] South Carolina,[4] Montana,[5] California,[6] and Arizona.[7] It is not only state and federal governments that are concerned about a right to privacy; individuals and families are also concerned. U.S. Supreme Court Justice Louis Brandeis summarized the principles underlying the constitutional guarantees of privacy:[8]

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.[9]

---

1 David Banisar, *The Right to Privacy as Customary International Law*, 1 (Privacy International Briefing Paper 1993) citing, *Entick v. Carrington*, 1558-1774 All E.R. Rep. 45.

2 HI Const. art. I, § 6.

3 WA Const. art. 1, §7.

4 SC Const. art. I, § 10.

5 MO Const. art. II, § 10.

6 CA Const. art. I, § 1.

7 AZ Const. art. 2, § 6.

8 M. Soler, A. Shotton, J. Bell, *Glass Walls: Confidentiality Provisions and Interagency Collaborations*, 5 (1993) (Youth Law Center).

9 *Olmstead v. United States*, 277 U.S. 438, 478, 48 S.Ct. 564, 72 L.Ed 944 (1928) (Brandeis, J., dissenting).

The right to privacy is necessary for the preservation of all other rights, for without the expectation that citizens can pursue their interests, follow the affairs of the nation, and arrange their personal matters with protection from the harsh glare of unrestricted and unending publicity, neither political rights nor other personal rights guaranteed by the Constitution would be of much value.[10]

When individuals and families become involved with educational institutions that are funded through federal and state funds, they are asked to share private information about themselves.[11] This information may include Social Security numbers, records of immunizations, family income, or criminal convictions. Sometimes families and children can be the subject of investigation to determine eligibility or kinds of assistance or services needed.[12] Laws and regulations have been developed to protect individual privacy and ensure that personal information is disclosed only when and where necessary.

Hierarchy of Legal Requirements

Confidentiality provisions form a "hierarchy" of legal requirements. *Constitutional provisions* are the highest: when the Supreme Court holds that a certain matter is protected as private under the U.S. Constitution, that decision will apply to every person and agency in the U.S.[13] All statutes, regulations, and other provisions—which legally rank below the U.S. Constitution—must comply or be consistent with a Supreme Court decision. (Similarly, a state constitution would apply to every one in that state.)[14]

The next hierarchical consists of *statutes*. Generally, there are separate federal statutes that cover particular areas, such as education. Some federal statutes cover state and local agencies throughout the country that receive federal funding from those agencies. At this level, many countries have privacy commissions. These commissions establish a baseline of how to handle documents. Then, each relevant industry develops further guidelines on how to handle sensitive documents.

Below statutes are *regulations*. Regulations supply details which are not in statutes and are intended to provide the specifics behind the implementation of a statute.[15] Regulations can contain forms, releases, court orders, identification of agency representatives to contact, and other material used in implementing confidentiality provisions. The regulations may even provide information on who should get what information and when it should be released.

---

[10] M. Aultman, P. Wolfson, and M. Rotenberg, State of Ohio ex rel. *Beacon Journal Publishing Co., et al. v. City of Akron, et al.*, Brief for Amici Curiae Public Citizens and Computer Professionals for Social Responsibility in Support of Appellants (1993).

[11] *Glass Walls: Confidentiality Provisions and Interagency Collaborations*, 5.

[12] Id.

[13] *Glass Walls: Confidentiality Provisions and Interagency Collaborations*, 14.

[14] Id.

[15] Id.

The final two levels are *statutory privileges*, which are usually contained in state law, and *professional ethical standards*. While these do not have the force of law, they are established, accepted guidelines for practice.[16] A prime example of professional ethical standards is the Code of Fair Information Practices, which other countries have also adopted. The Family Education Records and Privacy Act has also implicitly adopted the Code, and proposed health care reform measures will follow these principles. The following are the five parts to the code.[17]

1. **Stop Data Misuse** - Personal information obtained for one purpose should not be used for another purpose without informed consent.
2. **Encourage Data Minimization** - Collect only the information necessary for a particular purpose. Dispose of personally identifiable information where possible.
3. **Promote Data Integrity** - Ensure the accuracy, reliability, completeness, and timeliness of personal information.
4. **Allow Data Inspection** - Notify record subjects about recordkeeping practices and data use. Allow individuals to inspect and correct personal information. Do not create secret recordkeeping systems.
5. **Establish Privacy Policies** - Establish and enforce an information privacy policy. Make the policy publicly available.

Data Sharing

Data sharing and data security are two topics that were reviewed in the report *Glass Walls: Confidentiality Provisions and Interagency Collaborations*. The research focused on the statutes and regulations for the states of California, Washington, Iowa, and New York. The following summarizes some of the report's findings in the two subject areas.

Within the hierarchy of the legal scaffolding protecting agency data, there is sometimes an allowance to transfer data between government agencies. There is a general policy trend towards sharing only information that is directly relevant to a particular agency's purpose.[18] Such caution stems from a growing realization that "more" information is not necessarily "better."[19] As more information is collected, there is a greater danger of information being released to inappropriate parties.[20] Collecting additional data may also create more work and expense for an agency having to maintain special files and additional maintenance work for employees.

---

[16] Id.

[17] *Computer Professionals for Social Responsibility and Privacy International, Code of Fair Information Practices* (1992). Adopted from recommendations of U.S. Privacy Commission (1977).

[18] *Glass Walls: Confidentiality Provisions and Interagency Collaborations*, 11.

[19] Id.

[20] Id.

Limited data sharing can have several advantages. First, it cuts down on the amount of filing and maintenance. Second, most individuals are willing to share information with a few agencies who need the information, as opposed to the entire government. Third, it reduces the probability that information will be given out inappropriately.

The concept of limited data sharing is not restricted to conventional manual or hard copy systems, but also extends to automated systems. Just because a system is automated does not mean that its memory should be a large repository for any and all information. By limiting data and data sharing, there is less of a chance someone could inappropriately access data and allow confidential information to be released.

It is illegal for any person to read another's electronic mail, voice mail, or other forms of electronic communications without permission or without a warrant.

Data Security

Various levels of security are necessary to ensure the safety of data, starting with the physical environment.[21] Procedures for a chain-of-custody can be developed for handling disks and tapes and keeping logs of where each disk and tape is located.[22] The next step is limiting access to the data once they are part of the computer system.[23] This can be done through special directories with special passwords or double passwords. Another step is using identifiers to mask the personal identity of individuals whose personal information is in the system. Each system can develop identifiers through initials, birth date, or last name.[24] The uniqueness of the identifier becomes critical to confidentiality. An additional level of security is achievable by requiring employees to sign a confidentiality agreement that prohibits the disclosure of this sensitive information, except to those who have a need to know.

Access to Computer Records and Systems

Generally, there is no difference in the level of protection between files that are stored or transmitted electronically and those that are stored in physical form. In general, it is illegal for an individual to use a computer that the individual does not have permission to use or to exceed authorization in what he or she does with that computer. Depending on the computer system, such an illegal use can either be a state or a federal crime. It is also unlawful to read another person's electronic mail.

Under the Computer Fraud and Abuse Act of 1984[25], it is unlawful for a person without authority to access a computer that is used by a federal agency or a bank, or one that is used in interstate commerce. Nearly every state has an equivalent law that makes it unlawful to access any computer in the state without permission.

---

[21] *Glass Walls: Confidentiality Provisions and Interagency Collaborations*, 11.
[22] Id.
[23] Id.
[24] Id.
[25] 18 U.S.C. 1030.

Electronic Mail

Under the Electronic Communications Privacy Act[26], it is illegal for any person to read another's electronic mail, voice mail, or other forms of electronic communications without permission or without a warrant. However, the authority of an owner or operator of a computer to review an employee's mail is unclear. While the law is clear for monitoring telephone calls for business purposes, it does not explicitly authorize monitoring electronic communications, including reading E-mail. There are two cases pending against private companies who read their employees' E-mail.

Thus, monitoring should only be done in the most limited circumstances, when there is a particular suspicion that a specific individual is doing an illegal act. If the monitor involves a government entity, a warrant should be obtained.

Overview of Major Federal Laws

Interrelationship of Three Laws

The Federal Education Records and Privacy Act (FERPA),[27] also known as the Buckley Amendment of 1974, is the core of federal legislation regarding the confidentiality of education records. FERPA bans all schools[28] supported by federal funds from releasing a student's school records, or any other personally identifiable information, without prior consent from the student.[29] FERPA furnishes the *minimum* standard for record protection; state or local laws and regulations may augment, but not weaken, FERPA protection. These state laws may even be applicable to schools that are not subject to FERPA regulations.

The next most important piece of legislation supporting data confidentiality is the Privacy Act of 1974.[30] The Privacy Act was created to safeguard an individual from an invasion of privacy in the domain of federal agencies. Under the Act, any federal agency or organization that collects, maintains, uses, or disseminates personally identifiable records is responsible for timeliness, accuracy, completeness, and relevancy of the records and for protecting against their improper use or legal disclosure. Data are to be kept with "such accuracy, relevance, timeliness and completeness as is reasonably necessary" to assure fairness to the person.

Another federal law that has strong impact on data confidentiality is noteworthy not for its protection of data confidentiality, but for its threat to data confidentiality. The Freedom of Information Act (FOIA) of 1966[31] gives individuals and third parties more rights of access to U.S. Government records than any other law. There are four excep-

---

[26] 18 U.S.C. 2510 et seq.

[27] USC 1232g(1993), regulations at CFR 99 (1993).

[28] For the purpose of this paper, the term *school* will apply to either a school or an institution.

[29] For the purpose of this paper, the term *student* will refer to any party that can legally access the files, either the student if the student is over 18 or attends a postsecondary institution, or the parent of a minor or a legally incapacitated student.

[30] USC 552(a).

[31] USC 552.

tions to FOIA that prevent a government agency from handing over records. As a general rule, if a record release would severely harm an individual or company or business, the record will not be released.

Law Coverage

All three laws, as well as state and local laws, do not apply to the same entities. FERPA applies only to schools receiving direct grant funding and excludes those whose students receive Pell grants or other types of assistance. While it protects student records, it does not protect employment records of school employees.

FOIA permits access to information held by the U.S. Executive Branch agencies, and defines "agency" as an entity with which the government is involved or over which the government has authority in decisions affecting its ongoing, daily operations. More importantly, however, FOIA does not apply to state or local records or schools. FOIA does not define "record," but refers generally to documents in possession of and controlled by the federal government, including information that comes out of Congress and ends up in an agency's hands. The Privacy Act applies to all federal agencies.

Many states have provisions protecting the privacy of student records, either as independent provisions or as exceptions to open record laws. In states without such independent provisions, courts have ruled that the states may use FERPA as the basis for regulations.[32]

Electronic vs. Physical Files

FERPA, the Privacy Act, and FOIA do not specify media of record storage or methods of record transmission. No legal difference exists between the level of protection afforded to physical files and those that are stored or transmitted electronically or in any other form. Most state laws have similar open definitions.

Enforcement of Regulations and Penalties for Violation

Different government agencies have the responsibility of enforcing these laws, and violation penalties vary. For example, the Secretary of Education is charged with monitoring FERPA regulations. Schools guilty of violating FERPA may have their federal funding revoked. The Department of Education is also in charge of establishing standards for recordkeeping procedures at institutions falling under FERPA's domain.

A student who believes a school has violated FERPA may file a complaint with the Secretary of Education. Complaints to FERPA may be personal (denial of access to one's individual records, refusal to correct inaccurate information, or disclosure without an individual's or parent's consent) or broad (failure to establish record access procedures, compile lists of records maintained, log disclosures, protect records from unauthorized

[32] *Sall v. State*, 602 A.2d 1247 (MD 1992).

disclosures, etc.). FERPA does not give the student an independent right to sue a school for unlawfully disclosing personal information. However, several courts have ruled that a student may sue the school in a federal court as a civil rights violation under the student's state interpretations of FERPA.[33] Additionally, a recent Supreme Court case decision may increase the likelihood of suits for monetary damages for FERPA violations.[34]

Less vague than FERPA in terms of violation penalties, the Privacy Act stipulates both criminal and civil penalties for violators. An individual who willfully violates the Privacy Act can be convicted of a misdemeanor and fined up to $5,000. Any party who knowingly or willfully obtains a person's record on violation of the Privacy Act also faces criminal penalties. Civil liability for willful or intentional acts includes court injunctions against further acts, damage awards of no less than $1,000, attorney fees, and other related costs. No one particular agency is formally in charge of enforcing the Privacy Act.

Federal agencies do not have to comply with information requests under FOIA if the information requested falls under one of the FOIA exceptions, such as information that has been classified properly according to executive order. FOIA disputes are usually settled in court. The 1981 Department of Justice Guidelines directed that when agencies were sued for nondisclosure, the Justice Department was to defend the agencies solely because there was a substantial legal basis for withholding the information. As of October 4, 1993, the Clinton administration rescinded these guidelines. The new guidelines direct the Justice Department to assume that disclosures are correct, and agencies will be defended only if it is reasonably foreseeable to the agency that disclosure could harm a protected interest and if withholding is necessary to comply with FOIA limitations.

School Policy on Record Access

Written Policy

Every school subject to FERPA regulation must adopt a policy on its implementation of the law. This policy must include the procedures for record inspection and correction as well as for disclosure notice and hearings. The policy must state that the school will not disclose personal information without prior written consent of a student, but that education officials will have access. The policy must also specify what data the school will release as directory information (see below).

The school's policy regarding FERPA must be in writing and copies of it must be available to all students. The school must also make the policy widely available in prominent locations.

---

[33] 42 US 1983 (1992). See *Krebs v. Rutgers*, 797 F Supp. 1246 (D.NJ 1992).

[34] *Franklin v. Gwinnet Co. Public Schools*, 503 US, 112 S. Ct 1028, 117 L.Ed.2d 208 (1992). The case allowed for monetary damages for the intentional violation of the Title IX of the Education Amendments of 1972. See Johnson, *Managing Student Records: The Courts and the Family Education Rights and Privacy Act of 1974*, 79 Education Law Reporter 1 (February 1993).

Directory Information

Directory information includes the name, telephone number, date and place of birth, field of study, and earned awards and degrees of students. No law requires the schools to release this information, and many schools do not. Courts have upheld the schools' right not to release directory information in response to requests under FOIA or open record laws.[35]

Many individuals prefer to keep directory information private to avoid situations such as harassing calls and telemarketers. Many students are unaware of the possibilities of such nuisances before they consent to the release of directory information.[36] A school is not required to tell students of the above described possibilities. Each year, the student must decide if his or her personal data will be included in the directory. If a school still wishes to publish directory information, FERPA requires the school to notify the student prior to publication and to have the student's affirmative permission to release personal directory information.

Record Correction

A student may correct or amend a record if the record is incorrect, misleading, or violates the student's right to privacy. A student has a right to a hearing before an impartial official in order to challenge a record's content for accuracy. At such a hearing, the student has the right to have legal assistance or representation and to present evidence to justify allegations of record inaccuracy. Decisions from such hearings must be written and based solely on evidence presented at the hearing. If the student's request to correct or amend a record is denied, the student has the right to include a statement in his or her record stating why the student believes the information is incorrect, misleading, or an invasion of privacy.

Some schools are now considering the adoption of a record policy modeled after record maintenance practices currently used by the credit industry. This practice is to provide every individual with a free copy of his or her record for each year when changes are made to the record. This practice ensures record accuracy.

Posting Student Information

The posting of student test scores or other personal information (with the exception of directory information) using student names or Social Security Numbers as personal identifiers is in direct violation of FERPA. Schools may post personal information using a randomly generated identifier known only to the educator and the individual student.

Dissertations

All theses are considered education records under FERPA. However, the Department of Education determined recently that because theses are submitted for publication, any

---

[35] *Krauss v. Nassau Community College*, 469 N.Y.S.2d 553 (sup. 1983).

[36] See *Kestenbaum v. Michigan State University*, 294 N.W. 2d 228 (1980), *Krauss v. Nassau Community College*, Supra.

such document in written form implicitly provides a sufficient waiver to FERPA for undergraduate and graduate theses. The Department found that current university policies were sufficient. The question of dissertation publication without explicit student authorization as a FERPA violation was brought up by a school librarian's question to the Department, and not in the context of a complaint. However, one approach to clarify this technicality to avoid future legal problems is to require every student to submit a standard written waiver as an attachment to his or her thesis at the time of its submission.

Student Record Access Rights

Under FERPA, any student has the right of personal school record access if:

1. The student is over 18 years old; or
2. Is of any age and attends a postsecondary institution.

The student is entitled to explanations of the records' contents. Only students who have attended the school possessing the records are entitled to access their own records. For example, this excludes a student who had applied for admission to a school but was never accepted or never attended.

The only records that the school is not obliged to disclose to the student are financial records of a student's parent or confidential records that the student has expressly waived the right (in a signed statement) to see. This waiver must not be a requirement of admission to the school, and the records may only be used for the purpose for which they were intended. These documents are usually letters of recommendation for admission, employment applications, and honors or awards. The student still may revoke the waiver in writing.

FERPA does not explicitly mandate the student's right of access to medical or other records created while the student attended the school, nor does it prevent a physician or other qualified professional from viewing these records. Since the Act's passage, however, individuals have generally been granted the same access rights to their own medical records.[37]

The school may reserve the right to charge a reasonable fee for supplying a record copy to the student.

Notification of Student Rights

Each year, every school must notify every student of student rights under FERPA. The notice must include a statement of: the student's rights to inspect, review, and correct records to ensure that they are not inaccurate, misleading, or in violation of the student's right to privacy or other rights; the student's rights to consent to have his or her records

[37] See Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information*, U.S. Government (1993).

disclosed and those exceptions when consent is not necessary; the student's right to file a complaint with the Department of Eduction for a school violation of FERPA; and locations where students may obtain copies of the school's FERPA policy. The notice must be disseminated in a way to reasonably ensure that students are aware of their rights. Ideally, notification copies are disseminated to all students upon class registration or at other times when school materials are disseminated to all students early in the school term.

Third-Party Record Access Rights

FERPA allows any parent of a student under 18 access to the student's records. At the discretion of each postsecondary institution, a parent of a child who is over 18 may have access to the student's data if the student is still a "dependent" as defined by section 152 of the IRS Code of 1954. Otherwise, FERPA prohibits the dissemination of personal information to third parties, albeit with several exceptions.

Any disclosure must be made on the condition that the information will be kept confidential, unless disclosure is authorized, and that the information will be used only for the purpose under which is was acquired.

A third party may also gain access to student records with the student's consent. This consent must be in the form of a signed statement. The statement must specify the records to be released, explain the reason for release, and identify the party or class of parties who may receive the records.

Exceptions to Third Party Record Releases

Statistical Information

Student records that do not include personal identifiers may be released for statistical purposes. Anyone reviewing these records should not be able to associate the statistical information with a particular person. For a record to be considered statistical, all personal identifiers (e.g. name, address, Social Security Number, etc.) must be removed.

Educators

Some exceptions to the disclosure restrictions pertain to several classes of officials in the education field. These are:

1. Local education personnel who have legitimate educational interests in the student's data.
2. Other schools where the student is enrolled or seeks to be enrolled. Such disclosures must be reported to the student unless the student initiated the disclosure.
3. Certain federal, state, and local educational authorities (including the Secretary of Education and the U.S. Comptroller General) who enforce legal requirements in federally supported education programs. In such cases, personal identifiers

must be destroyed when work is completed, and only authorized officials may see the data before personal identifiers are destroyed. Courts have ruled that this exception has narrow application and is intended mainly for state and local education officials.[38]

4. Officials in charge of granting financial aid to students requesting financial aid. Disclosure purposes are for determining eligibility, amount of aid, conditions of aid award, and enforcement of award terms and conditions.

Testing and Accreditation Institutions

Schools may release student records to organizations that develop, validate, or administer predictive tests, student aid programs, and school improvements. Record releases may also be granted to accreditation organizations in order to carry out accrediting functions. Disclosure is allowed on the conditions that only members of the accreditation organization view the records, that resulting studies do not identify any particular student, and that personal identifiers are destroyed.

The Senate Report for the 1974 Privacy Act noted that "the extensive use of Social Security Numbers as universal identifiers in both the private and public sectors is 'one of the most serious manifestations of privacy concerns in the Nation.' "

Law Enforcement Records

Under a FERPA amendment established by the Higher Education Act of 1992, records created by a law enforcement unit for law enforcement purposes would not be subject to FERPA disclosure restrictions. This means that law enforcement-related student records kept by all levels of schools would not necessarily be confidential. In general, law enforcement records kept by schools relate to investigations of students who allegedly violated state or federal crimes. Other state laws and regulations concerning the disclosure of criminal records may also apply. A federal regulation defining this exception is currently under review.[39]

Records of Disciplinary Actions

Records of disciplinary records for student violations of school rules are considered confidential school records under FERPA. The Student Right to Know and Campus Security Act of 1990 created two exceptions:

1. A victim of a crime of violence may find out the results of a postsecondary institution's disciplinary actions against the alleged perpetrator of that crime.

2. A victim of sexual assault may find out the results of a postsecondary institution's disciplinary actions against the alleged perpetrator of that crime.

---

[38] *The Board of Education of the City of New York v. Regan*, 500 N.Y.S.2d 978 (Supp 1986). The chief financial officer of state, not the *de facto* education officer, is entitled to get a list of names suitable for special programs.

[39] See 58 *Federal Register* 62,298 (December 14, 1993), comments due by February 14, 1994.

Court Orders and Subpoenas

A school may disclose personal information without the prior consent of a student in order to respond to a lawfully-issued court order or subpoena. The school must notify the student prior to such a disclosure, and the student often has the right to challenge the disclosure, so it is not automatic. Many courts have used a balancing test between the interests of the disclosure and the privacy interests of the student.[40]

Emergency Situations

A school may release records in the event of a specific health or safety emergency. The Department of Education has stated that such emergency situations must be strictly construed.

Use of Social Security Numbers (SSN)

In 1992, students at Rutgers University successfully obtained an injunction from a federal court to prevent the dissemination of their SSNs on class rosters and identification cards. The court ruled that the dissemination of SSNs was a FERPA violation, was unnecessary, and was not related to legitimate educational interests.[41] Based on this court case, under FERPA, the SSN is considered to be personal information and a part of a student's education record, and its dissemination is prohibited.

Section 7 of the Privacy Act regulates SSN use among all federal, state, and local governments, including schools. The Act generally prohibits government agencies from collecting and disclosing the number, with the exceptions of disclosures authorized by federal law or disclosure practices adopted by a federal, state, or local law or regulation prior to January 1, 1975. The Act also prohibits agencies from denying any right, privilege, or benefit to any individual who refuses to disclose his or her SSN. Therefore, except for legal obligations, such as processing student loans, schools may not want to collect student SSNs. Schools do not need to use SSNs as student identity numbers or place them on student identification cards.

A state or local government may require SSN disclosure only to establish the identity of any person affected by a tax law or general public assistance law.[42] When an agency requests the disclosure of SSNs, the agency must provide written notice to individuals as to:

1. Whether the disclosure is mandatory;
2. The authority under which it is asking for the SSNs; and
3. The uses for which the SSNs are being requested.

---

[40] *Zaal v. State*, 602 A.2d 1247 (MD 1992).

[41] *Krebbs v. Rutgers*, 797 F. Supp. 1246 (D.NJ 1992).

[42] Tax Reform Act of 1976, Pub. L 94-455, Section 1211, 42 USC § 405 (c)(2)(c).

Privacy Concerns Regarding the Use of the SSN

SSNs facilitate the matching of different databases about individuals and can lead to invasions of privacy. The Senate Report for the 1974 Privacy Act noted that "the extensive use of Social Security Numbers as universal identifiers in both the private and public sectors is 'one of the most serious manifestations of privacy concerns in the Nation.'"[43] In 1993, the Federal Court of Appeals for the 4th Circuit ordered the Commonwealth of Virginia to stop disclosing citizens' SSNs when they register to vote because of the dangers this practice presents to privacy, and because of the increased vulnerability to fraud infringes on the citizens' voting rights.[44]

Recently, Congress's Office of Technology Assessment reiterated these warnings about the threat to privacy from widespread dissemination of SSNs:

> Concerns about the proliferation of the use of the Social Security number for purposes unrelated to the administration of the Social Security system, and the power of the number to act as a key to uncovering and linking a vast amount of information held by both the government and private companies, have been voiced in a number of contexts... As a result of this increased use of the Social Security number, the number now facilitates the ability of large institutions to compare databases. It allows outsiders (including private detectives, computer "hackers," or other strangers) to move from database to database, from credit bureau to insurance company to grocery store to publisher, to find out detailed marketing, financial, and medical information about an individual, so that a very detailed dossier on the individual can be created.[45]

SSN Use and Fraud

The use of SSNs increases the chance for invasions of privacy and fraud. The widespread use of SSNs is responsible for tens of millions of dollars in fraud each year. For example, individuals obtain SSNs of other individuals in order to retrieve credit reports from credit bureaus, and use the credit report information to illegally obtain credit cards and loans in the other individuals' names.[46] The widespread use of SSNs on campuses only facilitates this fraud by making SSNs easier to obtain.

The SSN As an Identifier

From a practical standpoint, the SSN is not a very accurate or reliable identifier. The SSN provides no "checksum" (an internal verification of the validity of the number). Thus, there is no way to ensure that the number is correct. Incorrect numbers can be

---

[43] S. Report No. 1183, 93rd Congress, 2nd Sess. (cited in *Krebbs v. Rutgers*).

[44] *Greidinger v. Davis*, 627 F.2d 494 (4th Cir. 1993).

[45] Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information* 64-65 (1993), cited in amicus brief of Public Citizens and Computer Professionals for Social Responsibility, *State of Ohio ex rel. Beacon Journal Publishing Co., et al. v. City of Akron*, No. 93-2012 (Supreme Court of Ohio, 1993).

[46] Neuffer, "Victims Urge Crackdown on Identity Theft," *Boston Globe*, July 9, 1991, at 13, 20; M. Quint, "Bank Robbers' Latest Weapon: Social Security Numbers," *New York Times*, September 27, 1992 at 7; Y.

entered intentionally or unintentionally. The Social Security Administration estimated that there are over 12 million SSNs currently being used incorrectly. The creation of a new identity number for students is a simple process, easily done on computer. School-generated identification numbers can prove more useful than SSNs, indicating information encoded within the number relevant to the status of the student.

SSN use also makes student record access easier. One of the facts considered during the Greidinger case was that a friend of the plaintiff was able to call up the University of Maryland and obtain Greidinger's student records by simply giving his SSN (the number was available as a public record as a condition to vote). Thus, the possession of a SSN should not be considered as evidence of a person's identity, especially when provided over the telephone.

Conclusions

Based on our legal research and interviews of experts, we found that various generic steps can be taken to protect a student's or employee's records, notwithstanding the wide variety of statutes and regulations at both the federal and state levels. These laws, regulations, and statutes address a broad array of data confidentiality, privacy, and access issues, some in more detail than others. Because there is such a broad array of issues to be addressed, some states do not even address certain privacy issues.

It should also be noted that Senator Paul Simon introduced a bill in December 1993 to the Labor and Human Resources Committee for the establishment of a privacy commission whose purview would cover all government branches. The intent is that this commission could establish a baseline by which all government agencies would have to handle data. A specific agency, if need be, could then develop guidelines germane to that agency. One reason for this proposed action is that data privacy is still a very new area of the law from a regulatory and case law perspective.

Lastly, based on the diverse array of material we researched and summarized in this report, the Forum may want to consider creating a "central database," or "clearinghouse," on relevant information and the latest developments in this issue area at the federal and state levels. The Forum could also:

1. Provide overviews and suggest standards and guidelines to federal and state officials;
2. Help foster consistency in how issues are addressed; and
3. Guarantee that key education officials are aware of relevant laws and regulations.

II. Matrix

The following matrix includes relevant federal laws, statutes, and regulations which deal with privacy and confidentiality. We have reviewed the list provided by the Forum and incorporated the appropriate laws, statutes, and regulations. We have expanded that list and included other agencies which address privacy and confidentiality.

The matrix describes what information can be released from a file, to whom information can be communicated, as well as what information can be communicated, if consent is needed, and how private information can be released other than through consent.

FEDERAL STATUTES AND REGULATIONS

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Aid to Families with Dependent Children (AFDC)	42 USC § 602(a)(9); 45 CFR § 205.50	Information concerning applicants of recipients (including names and address, social and economic conditions, medical data, agency evaluation of recipients; and amounts of assistance.) Name or address of any applicant or recipient to any federal, state, or local committee or legislative body. Lists or names of applicants and recipients.	For purposes directly connected with: (A) administration of the program or the SSI program (e.g., establishing eligibility, determining amount of assistance, and providing services for applicants and recipients), (B) any investigation, prosecution, civil or criminal proceeding related to administration of the program, (C) administration of any other federal or federally assisted program providing cash or in-kind services on the basis of need, (D) an audit of the program by a governmental entity, (E) verification to Employment Security Agency or similar agency that an individual has been an AFDC recipient for 90 days or is a WIN participant, or (F) administration of the state unemployment compensation program. For financial audit of program by governmental entity. In state plan for assistance under Title I, IVA, X, XIV, or XVI (AABD) of Social Security Act, if state legislation prescribes conditions of public access to records of disbursement of funds and prohibits use of list or names for commercial or political purposes. State or local agency can disclose current address of recipient to law enforcement officer who provides Social Security number of recipient and demonstrates that recipient is a fugitive felon.	Yes	If subpoena issued for case record or agency representative to testify, court's attention must be called to regulations against disclosure of information.
Adoption Assistance and Child Welfare	42 USC § 671(a)(8); 45 CFR §§ 205.50, 1340.14, 1355.21, 1355.30	Same as AFDC	Same as AFDC	Yes	Same as AFDC

From *Glass Walls: Confidentiality Provisions and Interagency Collaborations*, 5.

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Alcohol and Drug Abuse	42 USC §§ 290dd-3, 290ee-3 42 CFR § 2.1 et seq.	Records or other information concerning any patient in a Federally assisted alcohol or drug abuse program (including identity, diagnosis, prognosis, and treatment).	Internal program communications. Communications that don't disclose patient identifying information. Medical emergencies. Court-ordered disclosures. Patient crimes on program premises or against program personnel. Research, audit, or evaluation. Child abuse and neglect reporting.	Yes—must include (1) name of the program, (2) recipient of the information, (3) name of the patient, (4) purpose or need for disclosure, (5) how much and what kind of information will be disclosed, (6) patient may revoke consent, (7) date the consent expires, (8) signature of patient, and (9) date consent is signed.	Qualified service organization agreement (QSOA) with outside organization providing services to the alcohol or drug treatment program.
Computer Matching and Privacy Prevention	5 USC § 552A	Any item, collection, or grouping of personally identifiable information about an individual—educational, financial, medical, criminal, employment— that is maintained by an agency. Identifiable information in a computerized matching program used (1) to determine eligibility or compliance with regulations of federal cash or in-kind assistance programs, by applicants, recipients, or service providers, or (2) to recoup payments or delinquent debts under federal benefit programs.	To officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties if required under § 552 (Freedom of Information Act). Routine use of the record for the purpose for which it was collected. To the Bureau of Census for carrying out a census. If the record will be used solely as statistical record, and is transferred in a form that is not individually identifiable. To the National Archives and Records Administration. To a governmental agency for civil or criminal law enforcement activity. To a person showing compelling circumstances of health or safety. To either house of Congress or any committee or subcommittee. To the Comptroller General. Pursuant to court order. To a consumer reporting agency.	Yes	Written agreement between the agencies specifying, e.g., purpose and legal authority for conducting the program; justification for program and anticipated results; description of records that will be matched, with starting and ending dates for matching; and procedures for notice to applicants and recipients, verifying information produced, retention, and destruction of identifiable records, ensuring security of records, and use of records provided.

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Early Intervention Program for Infants and Toddlers (Part H of IDEA)	20 USC § 1480(2); 34 CFR § 303.460	Personally identifiable information (incorporates regulations applying to FERPA).	Same as FERPA	Same as FERPA	Same as FERPA
Family Education Rights and Privacy Act (FERPA)	20 USC § 1232g; 34 CFR Part 99	Educational records which contain information directly related to a student and are maintained by an educational agency or institution. "Educational records" does not include personal notes or records of teachers or other school officials, records kept for law enforcement purposes by school security, records relating to school employees, records on postgraduate activities, or certain treatment records of students.	To school employees within local school system who have legitimate educational interest in records. To school officials in district to which student intends totransfer. To federal or state educational authorities. To persons responsible for determining eligibility, conditions, or compliance with terms for financial aid. To anyone required to receive information under state statute in effect prior to November 19, 1974. Educational research organizations, providing confidentiality is assured. Accrediting organizations. Parents of students who are dependents under Internal Revenue Code. Appropriate person in health or safety emergency. Directory information (name, address, phone, date and place of birth, field of study, activities, dates of attendance, degrees awarded, etc.).	By parents, or by students over 18 years of age or enrolled in postsecondary program. Written consent must specify records to be disclosed, purpose of the disclosure, and party to whom disclosure may be made.	Court order or lawfully issued subpoena.
Food Stamp Program	7 USC § 2020(e)(8); 7 CFR § 272.1(c)	Information obtained from food stamp applicant or recipient households.	To persons directly connected with administration or enforcement of Food Stamp Act, other federal assistance programs, federally-assisted state assistance programs for low-income individuals, or general assistance programs. To persons directly connected with programs required to participate in state income and eligibility verification system (IEVS). To persons directly connected with verification of immigrant status of aliens through the Systematic Alien Verification Entitlements (SAVE) Program. To persons directly connected to the Child Support Program of Social Security Act, and employees of HHS establishing or verifying eligibility for benefits under the Social Security Act. To employees of Comptroller General's Office, for audits. To law enforcement officials investigating violations of Food Stamp Act. Recipients of information must protect against unauthorized disclosure.	Yes	

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
Freedom of Information	5 USC § 552(a)(2); 45 CFR Part 5b	Act directs federal executive branch agencies to make records, opinions, manuals, and other documents available to the public, except for the following: identifying details that would constitute a clearly unwanted invasion of personal privacy; national security or foreign policy; internal personnel rules and practices exempted by other statute; trade secrets, confidential commercial or financial information; inter- or intra-agency communications that would not be available to the public; personnel and medical files; certain law enforcement records; records related to regulation or supervision of financial institutions; geological and geophysical information and data concerning wells; possible violations of criminal law; law enforcement information records; and FBI records pertaining to foreign intelligence, counterintelligence, or international terrorism.		Release to anyone requires request reasonably describing the records.	Lawsuit filed in U.S. District Court.
Juvenile Justice and Delinquency Prevention	42 USC § 5776	Program records containing the identity of individual juveniles gathered for purposes pursuant to the statute.		Yes	
Maternal and Child Health Services Block Grant	42 CFR § 51a.6	All information as to personal facts and circumstances obtained by the project's staff about recipients of services.	Medical audits by the Secretary of HHS. Disclosure in summary, statistical, or other form that does not identify particular individuals.	Yes	
Medicaid	42 USC § 1396a(a)(7); 42 CFR § 431.300 et seq.	Information concerning applicants or recipients, including names and addresses, medical services provided, social and economic conditions or circumstances, agency evaluation of personal information, medical data (including diagnosis and past history of disease or disability), information for verifying eligibility and amount of medical assistance payments, and information for identification of legally liable third-party resources.	For purposes directly connected with administration of the program, including establishing eligibility, determining the amount of medical assistance, providing services for recipients, and conducting or assisting in civil or criminal proceedings related to the administration of the program. Emergency situations (but agency must notify family or individual immediately after supplying information).	Yes	Subpoena
Runaway and Homeless Youth	42 USC § 5731	Records containing the identity of individual youths shall not be disclosed or transferred to any individual or to any public or private agency.			

STATUTE	CITATION	INFORMATION RESTRICTED	ALLOWABLE COMMUNICATIONS	RELEASE BY CONSENT	OTHER RELEASE MECHANISMS
School Lunch	42 USC § 1758; 7 CFR § 245.8	Publication, posting, or announcement of names of eligible children. Overt identification of eligible children by special tokens, tickets or by other means. Physical segregation of eligible children by separate dining area, serving line, dining area entrance, or time to consume milk or meals.			
Special Education (Part B of IDEA)	20 USC § 1412,1417(c); 34 CFR § 300.560 et seq.	Educational records (same definition as in FERPA).	Same as FERPA	Same as FERPA	Same as FERPA
Women, Infants, and Children (WIC)	42 USC § 1786; 7 CFR §246.26(d)	Information obtained from program applicants and participants.	Persons directly connected with administration or enforcement of the program, including those investigating violations of the WIC program. Representatives of public organizations designated by the chief state health officer which administer health or welfare programs that serve people eligible for the WIC program (the organizations may use WIC information only for determining eligibility of WIC applicants and participants for health or welfare programs, and for conducting outreach to WIC applicants and participants). The Comptroller General, for audits.		
Youthful Offender	18 USC § 5038	Records of juvenile delinquency proceedings.	To another court of law. To an agency preparing a presentence report for another court. To law enforcement agencies investigating crimes. To the director of a treatment agency or facility to which the juvenile has been committed by the court. To an agency considering the person for a position immediately and directly affecting national security. To any victim of the juvenile delinquency, or if the victim is deceased, to the victim's family. If a juvenile is found guilty of certain felonies on two separate occasions, the court shall transmit to the FBI the name, date of adjudication, court, offenses, sentence, and not that the matters were juvenile adjudications. (NOTE: Information shall not be released if requested for an application for employment, license, bonding, or any civil right or privilege.)		

III. Synopsis of Federal Laws

This section gives a brief discussion of the following six Acts:

The Privacy Act of 1974
The Family Educational Rights and Privacy Act (FERPA)
also known as the Buckley Amendment of 1974
The Freedom of Information Act (FOIA) of 1966
The Computer Matching and Privacy Protection Act of 1988
The Internal Revenue Code, Tax Reform Act of 1976
The General Education Provisions Act (§ 1-406)

Each Act is described in greater detail than in Section One. The descriptions address each Act in terms of who the Act affects, what it does for the affected party, and why it was developed.

General Education Provisions Act (§1-406)

Under this Act, the Secretary of Education is annually required to provide to Congress a report on the state of education in the U.S. This report not only gives statistical information in regard to education, but also the views of the Secretary on what he or she sees as critical needs in education.

In order to provide this report, the Secretary relies on the National Center for Education Statistics (NCES) for collection and analysis of education statistics.

NCES has the responsibility of developing and enforcing standards designed to protect the privacy of people in the collection, reporting, and publication of data. NCES is not required to protect the information of institutions, organizations, and agencies receiving grants from the federal government. No one who works for NCES may use any individually identifiable information, make any publication whereby the data furnished by any particular person can be identified, nor permit anyone to access the individual data other than authorized people. Any employee, either permanent or temporary, is sworn to observe the limitations imposed above.

NCES is allowed to provide transcripts or copies of tables and other statistical records. Furthermore, NCES can provide special statistical reports to state and local officials, public and private organizations, and individuals. NCES is to be open to ideas from state and local educational agencies on the development of new and useful education statistical analyses.

The Privacy Act of 1974

The Privacy Act of 1974 was created to safeguard an individual from an invasion of privacy in the domain of federal agencies. Under the Act, any federal agency or organization that collects, maintains, uses, or disseminates personally identifiable records is responsible for timeliness, accuracy, completeness, and relevancy of the records and for

protecting against their improper use or legal disclosure. Data are to be kept with "such accuracy, relevance, timeliness and completeness as is reasonably necessary" to assure fairness to the person.

A senior official from each data-collecting agency is to be charged with the responsibility of data confidentiality (although this stipulation is not enforced) and requires all government-collected information about Americans to be kept confidential.

Set up in the post-Watergate era, the Privacy Act technically limits data collection only to "necessary information," and permits only Americans and permanent residents to request records about themselves. The Act defines a record as any item, collection, or grouping of information about individuals that is maintained by an agency and that includes a personal identifier.

The law forbids the government to possess secret databanks (although intelligence and law enforcement agencies can exclude entire systems from individual access) and gives people the right to know what information is kept about them, who sees this information, and how it is used, and the right to correct the information if necessary. In order to accommodate the Privacy Act's stipulation to let people know and view information collected by federal databanks in a timely fashion, many federal agencies have converted paper data into electronic data. According to a GAO report in 1990, the act has inadvertently "increased opportunities for inappropriate or unauthorized use of information, and made it more difficult to...safeguard individuals' rights."

The Privacy Act forbids government agencies to share data with other government agencies or people outside of the government, and the agencies may not use data for purposes other than the purpose under which they were originally collected. Many situations, however, are exempt from these stipulations. These exemptions are: disclosures to Congress, to the Census Bureau, to the National Archives, and to criminal investigators; and for health and safety emergencies, statistical research, in response to court orders, and routine use. Routine use means using the data for reasons compatible with the original use intended for the data, and routine uses must be published in the *Federal Register*. Routine use exemption is broad and used often by government agencies.

A 1986 GAO report identified seven federal agency duties brought on by the Privacy Act:

1. Allowing individuals access to their own records;
2. Establishing safeguards to prevent unauthorized disclosures;
3. Setting up periodic reviews of record keeping practices and policies;
4. Training government employees;
5. Publishing notices of records systems;

6. Maintaining Privacy Act-related procedures and directives; and
7. Reporting on and monitoring agency participation in computer matching programs.

No one is charged with enforcing the Privacy Act, as is the practice in many European countries where one law exists to cover all kinds of personal information. There are minimal restrictions on government collection, use, and disclosure of personal information. The vague language has let the courts side with the government in much Privacy Act litigation.

The Family Educational Rights and Privacy Act (FERPA), also known as the Buckley Amendment, of 1974

Under the Family Education Rights and Privacy Act (FERPA), any student has the right of personal school record access at schools receiving funds from the U.S. Department of Education if:

1. The student is over 18 years old; or
2. Is of any age and attends a postsecondary institution.

Additionally, any parent of a student under 18 who attends an elementary or secondary school that receives U.S. Department of Education funds has access to the student's records. At the discretion of each postsecondary institution that receives U.S. Department of Education funds, a parent of a child who is over 18 may still have access to the student's data if the student is still a "dependent" as defined by section 152 of the IRS Code of 1954.

Data disclosure to others without parent or student consent is generally disallowed. The disclosure exceptions are:

1. To local education personnel who have legitimate educational interests in the student's data;
2. To other schools where the student is enrolled or seeks to be enrolled;
3. To certain federal and state educational authorities to enforce legal requirements in federally supported education programs (in such cases, personal identifiers must be destroyed when work is completed);
4. To officials in charge of granting financial aid to students requesting financial aid;
5. To state and local authorities who require the information by law;
6. To testing, research, and accrediting organizations under certain safeguards;
7. Pursuant to a court order or lawfully issued subpoena; and
8. In specific health and safety emergencies.

In states where laws guarantee student rights that are stronger than those guaranteed by FERPA, the state laws take precedence over FERPA. These laws may even be applicable to schools that are not subjected to FERPA regulations.

The Department of Education is in charge of enforcing FERPA and establishes standards for recordkeeping procedures at institutions falling under FERPA's domain. Complaints to FERPA may be personal (denial of access to records, refusal to correct accurate information, or disclosure without individual's or parent's consent) or broad (failure to establish record access procedures, compile lists of records maintained, log disclosures, protect records from unauthorized disclosure, etc.).

The Freedom of Information Act (FOIA) of 1966

The Freedom of Information Act (FOIA) of 1966 gives people more rights to U.S. government records than any other law; it even usurps the Privacy Act. FOIA guarantees that everyone in the world may obtain information held by the U.S. Executive Branch agencies. (NOTE: This does not apply to state or local records or schools.) Although FOIA does not define "record," it is generally accepted as referring to documents in possession and controlled by the federal government, including information that comes out of Congress and ends up in an agency's hands.

Under FOIA, agencies may withhold data:

1. That have been classified properly according to executive order;
2. That relate solely to the internal personnel rules and practices of an agency (e.g., an investigative manual);
3. That are specifically protected by another statute, but only if that statute mandates withholding, establishes particular withholding criteria, and refers to particular types of information (e.g., personal tax data or census data);
4. About trade secrets or privileged and confidential commercial or financial information;
5. That would be privileged information in civil litigation (e.g., attorney-client privilege);
6. Of personnel and medical files;
7. From certain law enforcement records;
8. Related to the examination, operation, or condition of certain financial institutions subject to federal regulation; and
9. Of geological and geophysical information.

However, all agencies must publish the following information in the *Federal Register:*

1. Agency description;
2. Description of data access procedures, including where records are held and who is in charge;

3. Description of agency's decisionmaking and functioning process;
4. Rules of procedure, description and location of forms for obtaining information, and instructions for all required documents, reports, or examinations; and
5. Rules of general applicability and agency policy.

Agencies must make available their final opinions made in particular administrative cases, statements of policy, and interpretations adopted by the agency that are not published in the *Federal Register.*

On October 4, 1993, President Bill Clinton and Attorney General Janet Reno announced the Clinton Administration's policies regarding the FOIA. These policy changes will increase public access to government information. Agencies are now directed to make disclosures of information whenever possible. Withholding information is no longer justifiable if the information could technically or arguably fall within an exemption, and all information must be disclosed unless it is reasonable that such a disclosure would harm one of the government or private interests under the Act.

Furthermore, the 1981 Department of Justice Guidelines have been rescinded; from now on, when agencies are being sued for nondisclosure, the Department will no longer defend them solely because there was a "substantial legal basis" for withholding the information. The Department will assume that disclosure was correct, and agencies will be defended only if it is reasonably foreseeable to the agency that the disclosure could harm a protected interest and if withholding was necessary to comply with FOIA. Future changes are likely, as the Administration continues to review the regulations implementing the FOIA and the Privacy Act of 1974.

The Computer Matching and Privacy Protection Act of 1988

This statute protects any item, collection, or grouping of personally identifiable information about an individual—education, financial, medical, criminal, employment—that is maintained by an agency. Computerized matching may use the data to 1) determine eligibility or compliance with regulations of federal cash or in-kind assistance programs by applicants, recipients, or service providers, or 2) recoup payments or delinquent debts under federal benefit programs.

The agency may release information:

1. To officers of employees of the agency which maintains the record who have a need for the record in the performance of their duties;
2. If required under FOIA;
3. For routine use of the record for the purpose for which it was collected;
4. If the record will be used solely as a statistical record, and is transferred in a form that is not individually identifiable;
6. To the National Archives and Records Administration;

7. To a governmental agency for civil or criminal law enforcement activity;
8. To a person showing compelling circumstances of health or safety;
9. To either house of Congress or any committee or subcommittee;
10. To the Comptroller General;
11. Pursuant to court order; and
12. To a consumer reporting agency.

Records may be released with the individual's consent. Release may also occur with written agreement between two agencies with specific cause, such as purpose and legal authority for conducting the program; justification for program and anticipated results; description of records to be matched with starting and ending dates of matching; and procedures of notice to applicants and recipients verifying information produced, retention and destruction of identifiable records, ensuring security of records, and use of records provided.

The Internal Revenue Code, Tax Reform Act of 1976

Under the code, tax returns and return information are to be kept confidential. This information includes the taxpayer's identity; nature, source, or amount of income; and anything else related to the return itself. As with federal records, tax information is subject to the Privacy Act.

Exemptions for data disclosure are:

1. When the taxpayer consents;
2. Upon written request from state tax authorities;
3. To individuals with a material interest, e.g., spouses, business partners, the administration of an estate or deceased taxpayer's kin;
4. To certain committees of Congress;
5. To the Departments of Justice or Treasury for tax law enforcement;
6. To federal investigators in nontax cases if they have a court order;
7. For statistical surveys;
8. To certain agencies under specific program goals, such as to track down parents who are delinquent with child support payments;
9. To the president by his request (all requests must be reported to the Joint Congressional Committee on Taxation); and
10. To attorneys who are screening prospective jurors in a tax-related case.

This code, however, does not apply to state tax agencies. States are only required to establish administrative safeguards for all information received from the IRS.

Privacy Act	
Confidentiality	All government-collected information about Americans must be kept confidential. Damages may be collected for willful or intentional violations of this law.
Access	Americans are granted the right to know what information is kept about themselves, who sees this information, and how it is used. Government agencies are forbidden to share information with one another or with nongovernment individuals (see exemptions below). Only Americans and permanent residents may request records about themselves. Data are to be kept with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary" to assure fairness to the person.
Security	Federal agencies are obliged to establish safeguards to prevent unauthorized disclosures, conduct periodic reviews of recordkeeping practices and policies, train government employees, maintain Privacy Act-related procedures and directives, and report and monitor agency participation in computer matchings. No one is in charge of enforcing the act.
Ownership	Data may only be used for the purpose for which they were collected (see exemptions below).
Use	A federal agency or organization that collects, maintains, uses, or disseminates personally identifiable records is responsible for timeliness, accuracy, completeness, and relevancy of the records for the protection against their improper use or legal disclosure. Data may only be used for the purpose for which they were collected. EXEMPTIONS: disclosure to Congress, the Census Bureau, the National Archives, and criminal investigators; for health and safety emergencies; statistical research; in response to court orders; and routine use (using the data for reasons compatible with the original use for which the data were intended. All routine uses must be published in the *Federal Register*). The Act technically limits data collection only to "necessary information." A record is defined as any item, collection, or grouping of information about an individual that is maintained by an agency and includes a personal identifier.

Family Educational Rights and Privacy Act (FERPA)

Confidentiality	
Access	Any parent of a student under 18, any student over 18, and any student in a postsecondary institution has the right of access to the student's record at schools receiving funds from the U.S. Department of Education. At the school's discretion, a parent of a student who is over 18 at such an institution may access the record if the student is still a "dependent" as defined by section 152 of the IRS code of 1954. Data disclosure to others without a parent or individual consent is generally disallowed, except: 1) To local education personnel who have legitimate educational interests in the student's data; 2) To other schools where the student is enrolled or seeks to be enrolled; 3) To certain federal and state educational authorities to enforce legal requirements in federally supported education programs (in such cases, personal identifiers must be destroyed when work is completed); 4) To officials in charge of granting financial aid to students requesting financial aid; 5) To state and local authorities who require the information by law; 6) To testing, research, and accrediting organizations under certain safeguards; 7) Pursuant to a court order or lawfully issued subpoena; or 8) In specific health and safety emergencies. The school may withhold personal notes taken by teachers. In states where laws guarantee student rights that are stronger than FERPA, the state law usurps FERPA. These laws may even apply to schools not subjected to FERPA regulation.
Security	The Department of Education is in charge of enforcing FERPA and establishes standards for record keeping procedures at institutions falling under FERPA's domain. Complaints to FERPA may be personal (denial of access to records, refusal to correct accurate information, or disclosure without individual's or parent's consent) or broad (failure to establish record access procedures, compile lists of records maintained, log disclosures, protect records from unauthorized disclosure, etc.).
Ownership	
Use	A wide range of information may be collected: grades, emotional development, social behavior, medical problems, learning problems, political and religious preferences, family members, physical appearance, hobbies and extracurricular interests, ethnic background, economic circumstances, attitudes towards teachers and other students, psychological test scores, criminal history, even personal secrets told to a teacher or counselor. Information may by objective (weight and height) or subjective (impressions of a teacher). Agencies (DHHS, DoD, DoJ, SEC, etc.) and government corporations (Amtrak, U.S. Postal Service, FDIC, etc.) may withhold data from the general public:

Freedom of Information Act (FOIA)

Confidentiality	1) That have been classified properly according to executive order; 2) That relate solely to the internal personnel rules and practices of an agency (e.g., an investigative manual); 3) That are specifically protected by another statute, but only if that statute mandates withholding, establishes particular withholding criteria, and refers to particular types of information (e.g., personal tax data or census data); 4) About trade secrets or privileged and confidential commercial or financial information; 5) That would be privileged information in civil litigation (e.g., attorney-client privilege); 6) Of personnel and medical files; 7) From certain law enforcement records; 8) Related to the examination, operation, or condition of certain financial institutions subject to federal regulation; and 9) Of geological and geophysical information.
Access	Everyone in the world may obtain information held by U.S. executive branch agencies (not applicable to state or local records, schools, White House staff, and Congress) that does not fall under one of the exemptions above. FOIA usurps the Privacy Act.
Security	
Ownership	Agencies must publish the following information in the *Federal Register:* 1) Agency description; 2) Description of data access procedures, including where they are held and who is in charge; 3) Description of agency's decisionmaking and functioning process; 4) Rules of procedure, description of and location of forms for obtaining information, and instructions for all required documents, reports, or examinations; and 5) Rules of general applicability and agency policy. Agencies must make available: 1) Final opinions made in particular administrative cases; and 2) Statements of policy and interpretations adopted by the agency that are not published in the *Federal Register.*
Use	Although "record" is not defined, it is generally accepted as referring to documents in possession and controlled by the federal government, including information that came out of Congress and ends up in an agency's hands.

Computer Matching and Privacy Protection Act

Confidentiality	Protects any item, collection, or grouping of personally identifiable information about an individual—education, financial, medical, criminal, employment—that is maintained by an agency. Adverse matches must be verified independently before any action is taken. Individuals must be given notice as well as time to react to the allegations.
Access	The agency may release information: 1) To officers or employees of the agency which maintains the record who have a need for the record in the performance of their duties; 2) If required under the FOIA; 3) For routine use of the record for the purpose for which it was collected; 4) To the Bureau of Census for carrying out a census; 5) If the record will be used solely as a statistical record and is transferred in a form that is not individually identifiable; 6) To the National Archives and Records Administration; 7) To a governmental agency for civil or criminal law enforcement activity; 8) To a person showing compelling circumstances of health or safety; 9) To either house of Congress or any committee or subcommittee; 10) To the Comptroller General; 11) Pursuant to court order; and 12) To a consumer reporting agency. Records may be released with the individual's consent. Release may also occur with written agreement between two agencies with specific cause, such as purpose and legal authority for conducting the program, justification for program and anticipated results, description of records to be matched with starting and ending dates of matching, and procedures of notice to applicants and recipients verifying information produced, retention and destruction of identifiable records, ensuring security of records, and use of records provided.
Security	
Ownership	
Use	Computerized matching may use the data to 1) determine eligibility or compliance with regulations of federal cash or in-kind assistance programs by applicants, recipients, or service providers, or 2) recoup payments or delinquent debts under federal benefit programs.

Internal Revenue Code, Tax Reform Act	
Confidentiality	Tax returns and return information are to be kept confidential. This information includes taxpayer's identity; nature, source, or amount of income; and anything else related to the return itself. As federal records, tax information is subject to the Privacy Act.
Access	Exemptions are: 1) When the taxpayer consents; 2) Upon written request from state tax authorities; 3) To individuals with a material interest, e.g., spouses, business partners, the administration of an estate or deceased taxpayer's kin; 4) To certain committees of Congress; 5) The Departments of Justice or Treasury for tax law enforcement; 6) To federal investigators in nontax cases if they have a court order; 7) For statistical surveys; 8) To certain agencies under specific program goals, such as to track down parents who are delinquent with child support payments; 9) To the president by his request; all requests must be reported to the Joint Congressional Committee on Taxation; and 10) To attorneys who are screening prospective jurors in a tax case. This code, however, does not apply to state tax agencies. States are only required to establish administrative safeguards for all information received from the IRS.
Security	
Ownership	
Use	

U.S. Department of Education Security Policy	
Confidentiality	Sensitive data processed by the Department's resources shall be properly safeguarded against accidental or malicious disclosure, alteration, destruction, or delay. Each application system shall be classified as either high, medium, or low in criticality and sensitivity.
Access	A personnel security program identifies and screens positions involved with design, storage, retrieval, access, and dissemination of data processed through the Department's systems. It is the responsibility of all facility security managers, with the assistance of the organization's POSSO and telecommunications or data communications officials, to provide effective protection of sensitive data transmission which includes: 1) Assurance that adequate telecommunication controls are operating in support of each application system using data transmitted over a network. 2) Verification that data communication controls function as specified.
Security	
Ownership	
Use	

IV. State Laws

The following is a compendium of various state laws on privacy and confidentiality.[47] Some state laws deal with education, some with health, and some with employment. The laws described for education include information revealed to a counselor or teacher; to whom records can be transmitted; when records can be transmitted; and what records can be transmitted. Health and employment laws deal with how records are to remain secure.

Arizona Rev. Statute § 15-151

Since 1974, school records have been considered confidential and professional, with access only to parents, professional staff, state and federal agencies (if the information is kept anonymous), colleges, pupils older than 18, and others on the parents' instructions. A parent has the right to attach a written response to any disputed item.

Deerings California Code Annotated, Ed. 1987

§ 626.11 (Penal Code)

Students in public institutions of higher education are entitled to the state constitutional right of privacy, and limits are placed on the use of evidence seized from student dormitories in violation of constitutional rights.

§ 49060

State law on access to and disclosure of student records conforms to federal law.

§ 49063 Notification of parents of their rights

Upon entering a school district, parents are to be notified of their rights in relation to review, record copies, and consent-to-release information in their child's student record. This only deals with students under 18 years of age.

§ 49064 Log of persons and organizations requesting or receiving information

A log of all individuals and organizations requesting or receiving information for a legitimate reason will be maintained.

§ 49069 Absolute right to access

Parents of children under 18 years of age have an absolute right to access of any and all of their children's records. This right applies to both public and private schools. The school district will not edit the file in any way. Upon written request, however, parents may correct or remove any information recorded in the written records concerning their child. Procedures are in place if there is a question as to the parents' request for removal of documents.

Anwar, "Thieves Hit Social Security Numbers," *San Francisco Chronicles*, August 30, 1991, at A1.

[47] Various state references are from *The Privacy Journal*, State and Federal Laws and Regulations on Privacy, by Bob Smith, 1992.

§ 49074 Release of directory information

Directory information can include information such as student name, address, telephone number, date and place of birth, major field of study, etc. Each school district shall adopt a policy identifying those categories of directory information which may be released to third parties. The district will also determine which third parties may have access to the information within the directory.

§ 49074 Right to provide statistical data in which no pupil is identified

If no pupil can be identified, a school district may release statistical data at its own discretion when such actions would be in the best educational interests of the district's pupils.

§ 49075 Access to records by any person with written parental consent

A parent has the right to provide written consent for an individual or class of individuals to review or receive student record information.

§ 49076 Access to records by persons without written parental consent or under judicial order

Generally, a school district is not authorized to give access to or give copies of pupil records to any person without parental consent or judicial order. A few of the exceptions are: school employees within the district, officials of other public schools where a child might be moving, federal agencies where the information is needed to support or evaluate state or federally supported educational programs, or state officials who are to receive specifically required reports under mandates adopted prior to November 1974.

Further, information can be reported to a person in connection with an emergency if the information is necessary for the protection of health or safety, organizations related to financial aid, or organizations conducting studies on behalf of the Department of Education. (This is not an all-inclusive list.)

Colorado Rev. Statute § 24-72-204

Unless contrary to federal law, schools may allow employers or law enforcement access to pupil records without parental consent.

Connecticut General Statute, Annotated 1987

§ 4-193 Agency's duties regarding personal data

Each state agency is required to follow regulations specifically set out in § 4-196, below, as well as any other state or federal statute or regulation of personnel files.

Each agency is also required to take reasonable precautions to protect personal data from physical threats (e.g., fire) as well as individual third-party requests.

An individual may review his or her record upon written request, or consent to give a third party permission to obtain access. An individual will also have the ability to correct any data upon request.

If a third party requests access to a file, the individual whose record is in question will be contacted concerning the request.

§ 4-196 Agencies to adopt regulations conforming to attorney general's standards
The attorney general will develop uniform standards which require each state agency to describe the general nature of the personal data system, maintenance of records, use of records, and distribution of records. The attorney general will also develop categories of personal data (such as confidential).

§ 31-128b Employee access to personnel files
This section describes the rights of an employee in a business, enterprise, or private organization. As described above, an employee has a right to inspect and correct his or her file upon written request.

§ 31-128f Employee's consent required for disclosure
"No individually identifiable information contained in the personnel file or medical records of any employee shall be disclosed by an employer to any person or entity not employed by or affiliated with the employer without the written authorization of such employee except where the information is limited to the verification of dates of employment and the employee's title or position and wage or salary..."

§ 31-128g Employee's right to obtain copies
As stated above, as with state agencies, employees of other organizations can obtain copies of his or her personnel file.

Delaware Code tit. 14, § 4111

Allows access only to government agencies unless there is parental consent; permits schools to grant parental access to their own children's records, and protects school personnel from lawsuits for recordkeeping abuses.

Florida Statute Ann. § 232.23

Records are open only to parents, courts, schools, school boards, and others whom the principal or parents may authorize.

Idaho Code § 9-203(6)

School psychologists and counselors are immune in court from disclosing information without the consent of the pupil.

Illinois Rev. Statute Ch.122, para 50-1

The Illinois School Student Records Act, effective March 1976, provides similar safeguards as federal law and requires drafting of regulations for public schools.

Iowa Code Ann. § 68A.7

Records of present and former pupils are regarded as confidential, to be released at the discretion of the county superintendent.

Iowa Department of Human Services

Some of the regulations indicate that confidentiality is in a gradation system. Information which can be directly linked to an individual should not be released outside of the Iowa government, whereas statistical data not linked to individuals can be released.

Further, individuals who work in the system are required to review confidentiality information and attest to the fact that the specific regulations in regards to confidentiality will be followed.

Kentucky Rev. Statute § 421.216

Counselor-student communications are privileged.

Louisiana

Attorney General's Opinion, January 31, 1974, proclaims that children have a right to privacy in schools and that their records are confidential.

Maine Rev. Statute Ann., tit. 20, § 805

Counselor communications are privileged.

Maryland

Maryland State Government Code Ann., § 10-616

Records relating to the biography, family, psychology, religion, academic achievement, and physical or mental ability of any student may be disclosed to the student or to education officials.

Maryland Educational Code Ann., § 7-410

Any written or oral statement made by a student to a professional educator when the student is seeking information for overcoming any form of drug abuse may not be used as evidence against the student in any proceeding. The teacher's, principal's, or counselor's observations during such consultations are not admissible either.

Massachusetts General Law, Annotated 1992

Chpt. 69, § 4 Compilation of statistics as to certain institutions

The state has provided that each school can compile statistics which are required by the federal office of education in relation to number of pupils and instructors, courses of study, cost of tuition, and general condition of the institution. Nothing is specifically stated to ensure that the data cannot be traced back to an individual.

Chpt. 111, § 70 Records of hospitals or clinics; custody; inspection; copies; fees (1993 pocket pt)

Records can be reviewed and copies by the patient, patient's attorney with appropriate written authorization, executor or administrator of an individual's estate, or attorney for executor or administrator. No other third party may have access to the record.

Chpt. 71, § 34A, D, and E

A school "shall, upon request of any student or former student...furnish to him a written transcript of his record." Further, "Each school committee shall, at the request of a parent or guardian of a pupil, or at the request of a pupil 18 years of age or older, allow such parent, guardian or pupil to inspect academic, scholastic, or any other records concerning such pupil." The state board is required to adopt regulations for the storage and destruction of pupil records.

Minnesota Statute Ann., § 13.32

Public school and university records on students are governed by the state Data Practices Act.

Mississippi Code, 1972, Annotated 1990, § 37-15-3

This code contains requirements for contents of records, definitions of a permanent record, definitions of a cumulative record, maintenance of the records, disposal of the record, and handling the transfer of records. The code does not indicate in any way what type of record security exists, who can and cannot have access, nor what should be secure information.

Montana Rev. Codes Ann., § 93-701-4

Counselor communications are privileged.

Nebraska Revised Statute 1943, Revised 1987

§79-4.157 and .158

Academic and disciplinary records are to be segregated; disciplinary records are to be destroyed at graduation if authorized by the state records board. Teachers, parents, and the pupil have access to records. Local school boards shall set student records policy.

§ 84-1207.01 Agency head; designate records officer; duties

This individual is responsible for overall records management within a state agency.

§ 84-1210 Administrator; records; maintain; temporary removal; inspection

The above-named administrator shall properly maintain essential records and duplicates. The administrator is to safeguard the documents to ensure that third parties cannot obtain copies inappropriately.

Nevada Rev. Statute, § 49.290 and .291

A privilege is recognized for counselor-pupil communications.

New Jersey Rev. Statute, § 18A:36-19

Permits outside access, although regulations may be somewhat limiting. Personnel are protected from legal action based on statements in the record.

New York

New York City - Regulation of the Chancellor

The purpose of these regulation is to set forth requirements governing student education. The regulations specify what type of data is allowed to be collected, what is to be part of a student's permanent record, who can access the file, and what is maintained and for how long.

As described for several states above, New York City allows access by parent, legal guardian, and student. Any access by a third party, outside another government agency, court order or subpoena, has to be obtained by consent from either the child (18 years or older), parent, or legal guardian.

As for access to computerized student data, the City is highly concerned about confidentiality. One security measure the City takes is to give employees individual access codes and passwords so that there is tracking of who accesses what files. Further there are specific directives (Mayoral Directive #81-2) which specifically outline the security measures to be taken with respect to electronic data.

North Carolina Gen. Statute, § 8-53.4

Counselor communications privileged.

North Dakota Cent. Code, § 31-06.1

Counselors are immune from disclosure.

Ohio Rev. Code, § 3319.321

There may be no release of files for profit-making activities. Disclosure with parental consent or to another school is permissible. Directory-type information may be disclosed.

Oklahoma Statute Ann. tit. 70, § 5-115

It is a misdemeanor for any teacher to reveal any information regarding any child obtained in capacity as teacher except as required in performance of contractual duties or as requested by parents.

Oregon Rev. Statute, § 336.195 and § 44.040

Parental access allowed; parents may see behavioral records only in conference with a professional. Records are regarded as confidential but may be released to anyone with "demonstrated interest in the student." Elementary and secondary school teachers' communications are privileged.

Rhode Island Gen. Laws, § 16-38-5

State law creates a misdemeanor for circulating a questionnaire, without approval of the state department of education and the local school committee, that is "so framed as

to ask the pupils of any school intimate questions about themselves or their families, thus trespassing on the pupils' constitutional rights and invading the privacy of the home..."

South Dakota Codified Laws Ann., § 19-2-5.1 and .2

Elementary and secondary school counselors' communications are privileged except in cases of child abuse. College and university counselor-student communication is also privileged.

Tennessee Code Ann., § 10-7-504

School records are confidential, except when compelled under legal process, or released for the safety of person or property. Outsiders are authorized to have access to pupil records for research, and a pupil may give consent for others to have access.

Texas Rev. Civ. Statute Ann. art. 6252-17a, § 3(a)(14)

Student records are regarded as confidential, to be released only upon request of educational personnel, a student, parent, or spouse.

Vermont Statute Ann. tit. 1, § 317(11)

There are limits on the release of school records except as required by federal law.

Virginia Code, § 2.1-342(b)(3)

The Freedom of Information Act allows access only to the student involved or, if under age 18, to his or her parents. Letters of recommendation are not included.

Washington Rev. Code Ann., § 42.17.310

Records of students in public schools exempt from public records act of the state.

Wisconsin Annotated Statute, 1991

§ 16 Disclosure of Information (Banks and Banking)

No information can be released on an account or electronic fund transfer except by the consumer, a third party related to the electronic fund transfer, a person authorized by law who can have access, by court order, by an attorney or accountant of the financial institution, or by written authorization of the customer.

A bank employee may not incorporate its electronic fund transfer system lines with any other system for the purpose of ascertaining the physical location of a customer using the system.

§ 118.125 Pupil records (Education, 1993 pocket pt)

Confidentiality:

"All pupil records maintained by a public school shall be confidential..."

§ 146.02(4) Confidentiality of tests and related information (Public Health)
Laboratory hygiene test results will be provided to the physician who will then provide the results to the parents or legal guardian. Testing information can be further used for statistical compilations, providing no reference is made to the identity of any individual.

§ 48.78 Confidentiality of records (Children's Code - General Provisions)
"No agency may make available for inspection or disclose the contents of any record kept or information received about an individual in its care or legal custody..."

The provision does, however, allow a transfer of information between an agency and another social welfare agency or law enforcement agency.

Appendix: Resources

Federal Laws, Regulations, and Statutes

The Privacy Act of 1974
The Freedom of Information Act (FOIA) of 1966 and its amendments in 1974 and 1986
The Family Educational Rights and Privacy Act (FERPA), also known as the Buckley Amendment of 1974
The Computer Security Act
The Tax Code § 6103
The Social Security Act
General Education Provisions Act
Department of Commerce Bureau of Labor Statistics
Department of Agriculture, Food and Nutrition Program
The Department of Education
- National Center for Education Statistics
- Office of Programming and Planning
- Office of Bilingual Education and Minority Language Affairs
- Office of Postsecondary Education
- Office of Educational Research and Improvement
- Office of Vocational and Adult Education

Department of Justice
Fair Credit and Reporting
Education Privacy: testing, psychological records, privacy

Books

Administrative Communications Systems Handbook, The Department of Education's, Office of Special Education
Biennial Report of the President on Implementing the Privacy Act, 1988-89, OMB
Compilation of State and Federal Privacy Laws, by Bob Smith
The Freedom of Information Act Guide, Department of Justice
Glass Walls, by the Youth Law Center
Implementation of the Computer Matching and Privacy Protection Act of 1988 for 1990, OMB
Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret, by Jeffery Rothfeder
Privacy: How to Protect What's Left of It, by Robert Ellis Smith
Records, Computers, and the Rights of Citizens, Department of Health and Human Services
Your Right to Privacy: A Basic Guide to Legal Rights in an Information Society, by Evan Hendricks, et al.

State Statutes

Cal. Educ. Code
Conn. Gen. Stat. Ann.
Del. Code Ann.
Mass. Ann. Law
Miss. Code Ann.
Neb. Rev. Stat.
Wis. Stat. Ann.

State Constitutional Provision for Privacy

Alaska
Arizona
California
Florida
Hawaii
Illinois
Louisiana
Montana
South Carolina
Washington

Case Law

Armstrong v. Cross: Whitehouse E-mail was infiltrated. Found to be illegal.

Child vs. Robert R. Spillane, et al. 1989: a school was allowed to disclose to the community that an unnamed HIV-positive child was enrolling in the district.

DOE 1988: Court said that the DOE had to meet a private library's request to access computer-stored nuclear information; to the extent the DOE component had records in a database and software capable of searching it, DOE had to conduct the requested search.

Fay vs. South Colonie Central School District 1986: noncustodial father has the right to see his child's report card.

Rios vs. Read 1977: FERPA-protected documents could not be disclosed automatically upon discovery without first weighing the privacy interests.

Spas vs. Wharton, et al. 1980: a university could withhold transcripts from a student who failed to pay tuition.

State of Ohio v. Akron: Social Security Number privacy at issue.

Yeager v. DEA 1982, and *Long v. IRS 1979*: a U.S. Court of Appeals decided that an agency did not have to use its computers to manipulate data so otherwise exempt data could be disclosed; however, using a computer's capabilities to delete exempt data from the computerized records did not constitute the creation of a new record and did not justify denying access to nonexempt information.

People Contacted

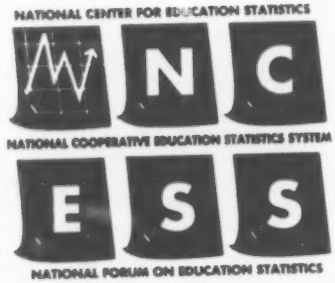
Sherri Alpert, IRS
David Banisar, Computer Professionals for Social Responsibility
Johanna Bonalick, Health and Human Services
Simon Davies, Privacy International
Pat Faley, Office of Consumer Affairs
Beth Givens, Privacy Rights Clearing Hours
Larry Hutcheson, Florida Department of Education
Tom McEntire, Department of Justice
Leroy Ruckaili, Family Policy and Compliance Officer
Margo Stevens, IRS
Rob Veeder, OMB
Peter Weatherdunn, OMB

ISBN 0-16-045075-6

90000

9 780160 450754

85


NATIONAL CENTER FOR EDUCATION STATISTICS
N C
NATIONAL COOPERATIVE EDUCATION STATISTICS SYSTEM
E S S
NATIONAL FORUM ON EDUCATION STATISTICS

NCES 94–635